Doctoral theses at NTNU, 2018:387

Juntao Zhang

Contribution to reliability and availability analysis of novel subsea technologies

Methods and approaches to apply in early design phase

ISBN 978-82-326-3562-7 (printed ver.)
ISBN 978-82-326-3563-4 (electronic ver.)
ISSN 1503-8181

NTNU
Norwegian University of Science and Technology

Juntao Zhang

Doctoral thesis

Doctoral theses at NTNU, 2018:387

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU
Norwegian University of Science and Technology

Juntao Zhang

Contribution to reliability and availability analysis of novel subsea technologies

Methods and approaches to apply in early design phase

Thesis for the Degree of Philosophiae Doctor

Trondheim, December 2018

Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering
Department of Mechanical and Industrial Engineering

ISBN 978-82-326-3562-7 (printed ver.)
ISBN 978-82-326-3563-4 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2018:387

Printed by NTNU Grafisk senter

Preface

Starting a PhD is probably the most important decision I have made. It is a deeply personal and long journey for training myself, both academically and psychologically. Along the way, there is full of ups and downs. There were moments that I was thinking about quitting PhD and finding a steady job so I can know what should I do. There were nights that I just faced my laptop, fuzzy eyes on the screen, and cannot come up with even one idea. There have been many 'detours' and 'off the tracks' before finally reaching the very end of this long journey. But all these frustrations and discouragements are paid by happiness of "light bulb" moments and compliments from someone I look up to, so I can keep a happy and optimistic mood to continue till the end.

Trondheim, Norway, September 2018

Juntao Zhang

Acknowledgement

This work was carried out as a part of SUBPRO, a research-based innovation center within Subsea Production and Processing. The authors gratefully acknowledge the project support, which is financed by the Research Council of Norway, major industry partners and NTNU.

First and foremost, I would like to thank my main supervisor, Professor Mary Ann Lundteigen, who has provided tireless guidance and professional supervision during the last three years. She shared with me her knowledge on RAM analysis from academia and industry, as well as experience on doing research. She devoted tremendous time on reviewing on papers and thesis, including late nights and weekends. She concerned my health and psychologic condition, and gave suggestions to my career development. Her working attitude and mindset really encouraged me. I would never have reached this point without her patience and professions.

I also profoundly thank my co-supervisor, Associated Professor Yiliu Liu, who has gave simulating insights, valuable ideas and insightful feedback to this work. I have learnt lessons from inspiring discussions with him.

I owe a great deal of thanks to many people who offered me constant help during this long journey. Here I would like to mention Professor Cecilia Haskins, Professor Antoine Rauzy, Professor Anne Barros, Dr. HyungJu Kim, for sharing their thoughts on topics of this work throughout daily discussions, internal seminars/workshops, and talks around coffee machine. Also thanks to my colleagues, Yun, Liu, Shenae Lee, Renny, Himanshu, Jon Martin, Aibo, Xiaopeng, Behnaz, Harald and many others, for joys and laughs we had together. It was a good experience to work with you.

I would like to thank for administrative staff of department of Mechanical and Industrial Engineering for the friendly working environment. A special thanks to the people of SUBPRO, especially to Gro Mogseth and Jon Lippe for their supports and instructions, and to Audun Faanes from Equinor as well as Andreas Hafver and Frank Børre Pedersen from DNV-GL for their detailed feedbacks on this work.

A special thanks to my friends in Trondheim, Mrs. Xiaolan Ma, Mr. Wei Guan and Mr. Qidi Wang, for friendship and happy moments together.

Last but not least, I would like to thank my family and friends, who gave me supports from the beginning to the end. Thanks for believing in me.

Abstract

Reliability, availability and maintainability (RAM) are considered as critical attributes for design and performance attributes of a product. Performing RAM analysis is an essential step to qualify the new product before it is released to the market and put into operation. RAM analysis is used to support the important decision making about inspection, maintenance and repair strategy, spare parts management, system architecture, remaining useful life and the like.

It is therefore important to perform a RAM analysis as early as possible, to ensure that any necessary redesign is made at a point where the consequence for costs is low. There are several constraints for RAM analyses in the early phase, such as e.g. limited data and information, the lack of detailed specification and a high level uncertainty. At the same time, RAM analyses could provide useful inputs, in particular where systems are becoming more complex, more integrated, and with more reliance on novel technology elements and system concepts. This may be an explanation why industry partners reported that RAM analyses are often introduced too late in new subsea system developments even if such methods could provide valuable input for the initial discussions about alternative design concepts. The main contribution of this PhD project consists of a new framework that guides RAM analysis and specific models towards this framework, considering complexity and novelty of new subsea design.

The starting point for this research was to investigate how RAM analysis can be better aligned with other engineering tasks. In this sense, a suitable approach is needed to communicate the system complexity when integrating RAM analysis in subsea design process. One central question was how to align RAM analysis better with the domain of Systems Engineering (SE), which is quite well established processes in many companies. RAM-SE framework proposed in this thesis represents an innovation that manages dialogue, used concept and produced models between SE domain and RAM domain.

In addition to the framework entails *what* are needed to carry out a RAM analysis in the early phase of a complex subsea design, more specific examples of contributions that details on *how* are as following:

- A proposal named STPA-RAM model to align dysfunctional analysis with RAM modelling and calculation. The major advantage is to quantify the hazards on controller-based systems with complex interactions that beyond the scope of traditional models used for dysfunctional analysis.

- A proposal for failure rate predication of novel subsea system, by assessing the impact of influencing factors relevant for subsea environment and operation. Compared to existing models, the proposal is based on Bayesian network to incorporate dependencies between influencing factors and allows to update the failure rate when design proceeds.

- A recommendation on selecting formalisms for RAM modelling, considering system dependencies, stage of development, nature of calculation and required mastery. It aims at improving one's understanding about how to construct an efficient RAM model for subsea system in the early design phase, considering the balance of simplicity and expressiveness.

- A review and evaluation of RAM allocation models, considering the subsea complexity issues like modularity. It aims at initiating further discussions among analysts and engineers having interests in reducing gap between the state of art knowledge and the need for allocation models used in subsea design.

This PhD thesis contributes to a closer collaboration between RAM analysts and system designers, since RAM analysts may, on the basis of discussions and results of this project, get a better understanding of how to give input and results that are more aligned with the needs of the designers. This work identifies limits of existing RAM practices associated with early design, and searches for improvements from a variety of appropriate and interdisciplinary theories and concepts. It provides practitioners with a guideline on RAM analysis in early design phase.

It is assumed that readers of this thesis are familiar with reliability theory, (e.g. book 'System Reliability Theory, Models, Statistical Methods, and Applications' by Rausand and Høyland), as well as and commonly-used models for RAM analysis. The knowledge and experience of subsea design and related standards are considered to be beneficial.

Table of content

List of figures and tables:

List of Figure:

List of Table:

Chapter 1 Introduction

This chapter presents an overview of this PhD project. It starts with a background to the research topic, including motivations and main research interests. The proper definitions for frequently used terms in this thesis are given, before presenting research questions and objectives. In the end, research approaches are presented and the structure of thesis is outlined.

1.1 Background

The subsea system has been an essential part in oil and gas (O&G) industry for past decades. It consists of many parts: production systems to explore and develop O&G field and produce hydrocarbon flow from the subsurface wells, processing systems to separate byproducts (e.g. water or other particles) from mixed flow and provide sufficient pressure to transport valuable product (i.e. oil and gas) to receiving facilities, and control systems to monitor and regulate the operation and process. Compared to topside (i.e. based on fixed or floating facilities) exploitations, the development in subsea technologies enables platform-less and unmanned production and processing, extends reach to remote and deep-water environment and improves productivity.

Norwegian-based O&G industry has been in the forefront of developing subsea fields and subsea technology over the last three decades. To maintain this position, it is important that the industries jointly seek solutions to accommodate new needs and new challenges for O&G activities. Several strategic efforts have been taken, for example *All Subsea* [1, 2] and *Subsea Factory* [3, 4]. One of the most recent achievements is the world's first gas compression system at Åsgard field, which started to operate the first gas since September 2015 [5]. It is reported that Åsgard gas compression system provides higher production rate, and reduces energy consumptions and carbon emissions. At the same time, global O&G industry faces critical challenges like the low oil prices at lower levels that have been in the past and the technology revolution on North American shale. The subsea industry therefore needs to provide more cost-efficient subsea solutions for flow assurance, control and instrumentation, installation and operation. A recent report from 'oil and gas in 21 century' (OG21) project points at some needs [6]:

- To make discovery economically viable in the more complex reservoir: deep-water, remote area from shore and challenging environment like arctic areas

- To reduce complexity of subsea system hardware and orient to more energy efficient, simpler and cleaner way to produce, process and transport oil and gas offshore.

- To develop the dedicated qualification program for new technology in subsea applications, so that the potential weakness and errors are removed before installation on seabed.

- To reduce cost in related to inspections and maintenance, and minimizes the associated interruptions and stops on the production and system integrity.

The mentioned subsea challenges have been the starting point for a new research-based innovation center in subsea production and processing called SFI SUBPRO started up by 2015. The new research center is the result of a joint effort by several research groups at NTNU and representatives from the O&G industry. The involved industry partners are:

- Equinor (former Statoil): from 2015- now
- Neptune Energy Norge AS (former ENGIE): from 2015-now
- DNV-GL: from 2015-now
- Lundin Norway AS: from 2015-now
- VNG Norge AS: from 2015-now
- ABB: from 2015-now
- Aker BP: from 03.2018- now
- Shell: from 2015- 01.2018
- Aker solution: from 2015- 01.2017

As shown in Figure 1-1, SUBPRO involves from NTNU side five research groups: field architecture, separation-fluid characterization, separation-process concepts, system control and reliability, availability, maintenance, and safety (RAMS). The number of project for each research group has been continuously increased since SUBPRO started up in 2015.

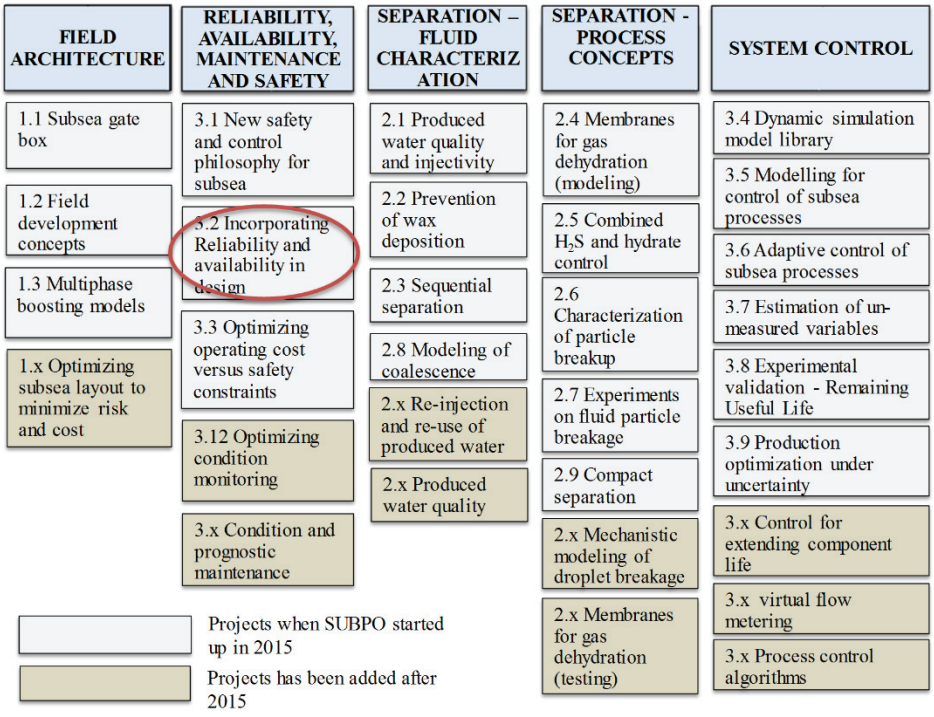


Figure 1-1 The project structure of SUBPRO

That RAMS was allocated as a separate research area was an evidence that the topic was of high interest for the industry partners as an enabler of innovations in subsea O&G sector. Reliability denotes the ability of an item to perform a specific function under given specified (i.e. environmental and operational) conditions and for a stated period of time [7]. Maintainability denotes the ability (i.e. the ease and speed) of system to remain in or restore to the functioning state [8]. Availability extends the definition of reliability by assuming the required external resources (e.g. maintenance supports) are provided [8]. Safety is defined as '*freedom from unacceptable risk*', and relates to measures for reliability as well as availability in cases where the system functions are safety-critical. The lack of RAMS performance has direct impact on system production, such as unplanned downtime due to critical failure and insufficient maintenance and loss due to environmental pollution and human injuries. The analysis of RAMS aspects helps end-users identify the potential deviations of operational performance against its intended gain and drives the work towards RAMS improvement in the design and operation phase. The thesis presented here corresponds to SUBPRO-subproject-3.2 "*incorporating reliability and availability in subsea design*" within RAMS research area as shown in Figure 1-1.

The subject of *safety* has not been a primary focus of this PhD research project. This does not mean that safety is not important, and safety *is* a key topic of another research topic in RAMS research area of SUBPRO. Ideally, there should be one reliability engineering team to handle both safety and RAM aspects, and cope with the conflicting of interests [9]. This PhD research project has concentrated on the analysis of reliability and availability performance of new subsea solutions which have been proposed to allow more flexible subsea production or reduced costs of design, installation, and operation. In this thesis, the term *RAM* is used to denote the aspects of reliability and availability, even if the research has not focused on maintainability as such. The influence of maintainability and maintenance are indirectly incorporated in the measure for availability, and as such it seems reasonable to suggest RAM as a suitable term. In this respect, RAM is an interchangeable term with dependability defined in IEC 60300 [10].

RAM analysis plays an essential role in the engineering design process to create competitive advantages, such as reducing investment and operational budgets, controlling the risk of redesign, and mitigating potential future production disturbances [11]. The purpose and process of RAM analysis are to answer two questions in order to support introduction of new technology:

1) What is RAM performance against overall performance target?

2) How to verify whether the RAM is achieved?

The answer to these two questions in the context of subsea design is the central element of this thesis, and given as a framework that describes the procedure of RAM analysis and necessary methods/models.

1.2 Definition of terms

It was recognized that precise definitions of key terms are worthy to support literature review and discussions for this research work. The selected terms may have several meanings across literature or may not have been defined generally in RAM community. Table 1-1 thereby presents to clarify their uses in this thesis, based on definitions recalled or adapted from international electro-technical vocabulary IEV-192 [12] and the related international standards (e.g. IEC 60300-3-1 [13] and ISO/TR 12489 [9]). The explanatory comments are added, if needed.

Table 1-1 Glossary of key terms

Terms	Definitions and explanatory comments
System	A set of interrelated elements that interact collectively to fulfill a certain set of functions. **Comment:** the term *element* refers to the part of a system, and covers hardware, software, human, and organization factors. The elements are in a certain form or following the same logic (architecture) with specific limits (environment and operation support). The unfamiliar or unintended interactions between elements lead to the difficulty of understanding a system (i.e. the complexity), which is discussed in section 3.2.
Framework	An overall conceptual structure that organizes and guide the analytical methods, tools and ideas to be applied in different works and contexts.
RAM analysis	A throughout process to characterize combinations of evolutions (e.g. degradation and failure) and maintenances (e.g. replacement and repair), and evaluate the associated consequences (deviations) on fulfilling required functions. **Comment:** the outcome of RAM analysis is supposed to support decision making about redundancy, modularization, strategies for interventions and the like.
Early design phase	A stage for concept development where many concepts are generated and evaluated at a high (functional) level and the details for realizing required functions are not settled. **Comment:** after applying RAM analysis in early design phase, only a few concepts (normally one or two) will be forward to *detailed design phase* that determines the details about architecture of elements to realize functions. The main steps of RAM analysis in early design phases are identified in section 4.2.
Model	A (graphical) representation, description or analogy of a system/element that cannot be directly observed. **Comment:** in this thesis, models that support the analytical work of a discipline are named after it, for example RAM models. Models are used to either communicate the certain understanding of a system, or play the virtual experiment of a system. Fulfilling the latter task means that the model is *executable*, which refers to the term presented next.
RAM (reliability) modelling	A model based on mathematical frameworks used for calculating or simulating of reliability measures. **Comment:** it should be noted that the term *reliability measure* here embraces a wide range of aspects, including reliability, availability,

	maintainability and maintenance supports. In this respect, the alternative term *RAM modelling* is preferred in this thesis. The formalisms for RAM modelling can be classified based on the nature of calculation (analytical calculation or simulation), or based on the nature of modelling that discussed in Chapter 8.

This research project produces two types of results: *models* and *frameworks*. New models are developed on the new theoretical basis (set of rules), or fusion with other domain-specific models to compensate the weakness of each model by their strengths. The new framework is to provide a new way to guide the preparation, construction and evaluation of recommended models. These innovations contribute to RAM analysis where the current frameworks/models are immature or insufficient in early design phase.

1.3 Problem statement and objectives

Manufacturers and system integrators of subsea systems use internally developed framework for RAM analysis, following production assurance standards such as ISO 20815 [14] and recommended practices such as DNV-RP-A203 [15] and API-RP-17N [16]. In discussion with industry, it is indicated that RAM analysis is mainly undertaken for demonstrating conformance to requirements, and reaches its limits in the early phase of complex subsea design. Introducing RAM analyses as early as possible can enable the early trade-off, thus significantly reduce the risk of costly corrections or even re-design in later phases. At the same time, the analyses are subjected to (at least) challenges stated as follow:

- The system design in the early phase of development is highly conceptualized for all engineering disciplines. A system concept may be found to be very abstract, as opposed to the detailed design phase where system has reached a level of detailing where simplifications need to be made for RAM analysis.

- The requirements for new design may often focus on giving boundaries of what is acceptable performance. In this sense, there is more than one design alternative to be considered in the early phase. The screening or selection must be made with confidence, as the concept selection, once made, can be difficult to reverse. It is therefore a dilemma that RAM analysis is needed early to make irreversible decisions, while the level of details about the concepts are still premature.

Besides, the complexity of subsea system becomes a main constraint for RAM analysis. Some complexity characteristics induced by new subsea technology or subsea environment may challenge commonly-used models for RAM analysis:

- The new subsea design may be subjected to complex interactions due to for example the compact and modular structure and introduction of computer control technology. RAM analysts may be unfamiliar with these complex interactions or lack proper tools to consider them, which leads to risk that some failures are overlooked in (the early phase of) subsea design.

- The limited accessibility to subsea field and acceptance to degraded operation imply dependencies on the operation of inspection, maintenance and repair (IMR), which have strong impacts on overall production performance and availability of system. These impacts cannot be quantified through the commonly used models like fault tree.

Given the aforementioned problems, the main objective of this thesis can be stated as:

> ***'Enable more efficient use of RAM analysis in the early design of subsea systems, considering aspects of novelty and complexity.'***

There are many considerations that are relevant to ensure this enabling. Two have been identified as of particular importance: The *integration* of RAM analysis team with systems design team, and the need to make RAM analysis *useful*, despite that concepts in an early design phase are specified at a high (functional) level. For this PhD research, the following two sub-objectives were therefore formulated:

Sub-objective 1: To propose a framework that incorporates results and indications from different expertise domains in subsea design, ensuring that the system concept is communicated correctly and that the correct system concept is communicated.

Two expertise domains are mainly focused in such framework: system designers who are in charge of designing Systems Engineering (SE) models to anchor various discipline engineers (e.g. mechanical and electronic) in maturing subsea design concept, and RAM analysts who evaluate RAM performance for defined system concept and provide recommendation. The exchanges of information and constraints between these two domains are identified as sparse

in present industry practices. This requires a new framework to unify the force and artifacts of each domains.

To meet sub-objective 1, the proposed framework, denoted as RAM-SE framework, will at least handle following issues:

- Review the common SE and RAM models, and identify the overlapping areas and potential integration points between these two expertise domains.

- Evaluate the advancement of applying SE models on enriching the models used in RAM domain.

- On basis of elaborations for first two issues, establish the concurrent design review about how RAM recommendations are considered in the joint evaluation of a design.

The new knowledge and improved models are introduced to make RAM analysis suitable in subsea context. That is, the second sub-objective of this thesis.

Sub-objective 2: To develop, propose and suggest new models for RAM analysis, which are suitable for top-down analysis (preferred in early phase) and the treatment of uncertainty/lack of knowledge (dealing with increased complexity).

In early design phase where the realization of system is not mature, RAM analyst focuses on revealing the potential failures of design concept, and assessing the consequence of critical failure considering the associated countermeasures and maintenance strategies. As such, several tasks are oriented to complete a RAM analysis. First is to formulate requirement on basis of standards, regulation and business needs, and allocate to lower level of system, e.g. subsystems and components. The next is to understand what can go wrong for selected system level, i.e. dysfunctional analysis. Afterwards, it is needed to collect data to estimate frequency of critical failures and hazardous scenarios, i.e. failure rate predication. The final step is to accomplish the calculation and simulation through selected modelling formalism thus give quantitative indicators about RAM performance. Considering the novelty and complexity of subsea system, the proposed models for these tasks will at least handle following issues:

- The model for RAM allocation should consider some aspects of interest for subsea design, e.g. modularity of subsea system and group maintenance strategy.

- Given the situation that subsea system is being more intelligent and more dependent on software, dysfunctional analysis must be able to reveal the hazards and failure caused by complex and software-intensive subsea operations.

- The increase in the complexity of a subsea system implies that it may be owing to a higher number of failure mechanism, which can be influenced by several factors including operational loads, manufacturing and design and operating environments. A practical model for failure rate prediction must be provided in early design phase.

- A complex subsea system with specific features such as dynamic properties requires the advanced modelling formalism, which in turn increases computational time and requires higher competence of analysts. The selection of formalisms for RAM modelling must consider the balance of expressiveness and simplicity, and give the explanatory comments when the feasible modelling formalism cannot be used due to practical constraints.

1.4 Delimitation

The PhD research documented in this thesis has following delimitations.

First, this research work contributes to develop a suitable RAM analysis as a foundation to support decision-making of subsea design. The methods and models for decision-making itself (e.g. analytic hierarchy process) is not the main focus in this research work.

Second, the insights from the manufacturer perspective are superficially included in this research work. The manufacturers from subsea industry have shared few details about their internal procedures and practices about RAM analysis. In addition, as the market declines some of manufacturers withdraw from SUBPRO in the beginning phase of this research project. It gave less opportunity to verify and improve some results of this research work.

Third, the review and investigation of current RAM practice in subsea design are mainly based on recognized standards and guidelines, where the access to industry practices is limited. This situation also implies some limitations of the presented works. For example, the adopted practices and standards for design of subsea production system are mainly ISO 13628-1 [17], API-RP-17N [16] and NORSOK U-001 [18]. One limit is that the above standards do not cover requirements of subsea processing systems. In addition, O&G industry adopts

standard ISO 20815 [14] as guideline for RAM practice, but it is not subsea specific. As compensation to this limitation, the thesis focuses on generic standards for RAM analysis like IEC 60300 [10] and also presents lesson learnt from other sectors such as SAE ARP4761 [19] for aviation and EN50126 [20] for railway. The sector-specific considerations are taken into account when adapting the existing RAM practices for subsea design.

Finally, case systems elaborated in this thesis are highly conceptualized and have a large potential to change and revise in future. For instance, the main case system in this thesis is provided internally from SUBPRO, the subproject 1.1 "subsea gate box". To demonstrate the applicability of the proposal in this thesis, some assumptions and simplifications are made to abstract the core idea of the given design concept. The conflicting interests and the focus of case study are jointly discussed and agreed by the author and subproject 1.1.

1.5 Research approaches and structure of thesis

A research work can be viewed from many different perspectives. One classic perspective is to divide the research into *conceptual* and *empirical* [21]. A conceptual (or *theoretical* preferred by some researchers) research relies on developing new concepts/theories or modifying existing concepts/theories to solve the emerging problems, whereas an empirical research relies on collecting evidences/data from experiments and observations. From this point of view, this research work is characterized as conceptual, since this research work mainly contributes to adapting other disciplines and integrating existing models to improve the usefulness of RAM analysis in the early phase of a new subsea design.

Given the different purposes of research, a research work can also be *fundamental* and *applied* [22]. A fundamental research is mainly concerned with generalization of theory for a rising research problem/field where few theory and concept are available. An applied research is driven by the practical problem to seek solutions from one or more disciplines. From this point of view, this research work is positioned as applied research. Before this research work, there exists a branch of state of art documents related to RAM analysis, such as best practices, standards and guidelines. After literature review, they are recognized to be challenged by novelty and complexity of new subsea design. The research problems are formulated accordingly, and new theoretical basis and interdisciplinary models are implemented to propose new solutions.

This PhD thesis starts with a status and gaps analysis based on both academic and industrial perspectives. The status and gaps analysis was evaluated by SUBPRO, and several research topics were agreed in light of their relevance and

priorities. The research articles and course works have been prepared for each topic. Figure 1-2 illustrates the contributions related to each topic. Contribution I is associated with sub-objective 1, proposing a new framework that aims at bridging between design process and RAM analysis within the support of SE models. Contributions II to V concern RAM models, which are related to sub-objective 2. Contribution II is to propose a new model for revealing and assessing the dysfunctional behavior of controller-based and software-intensive subsea systems. Contribution III is to propose a new model for failure rate predication based on Bayesian network, using multiple sources of information (e.g. historical data, expert judgment and field experience). Contribution IV suggests and recommends selection criteria for modelling formalism about RAM calculation and simulation, considering the constraints posed by system complexity. Contribution V presents a review on methods for formulation and allocation of RAM requirement, and suggests necessary improvements regarding their uses in subsea context.

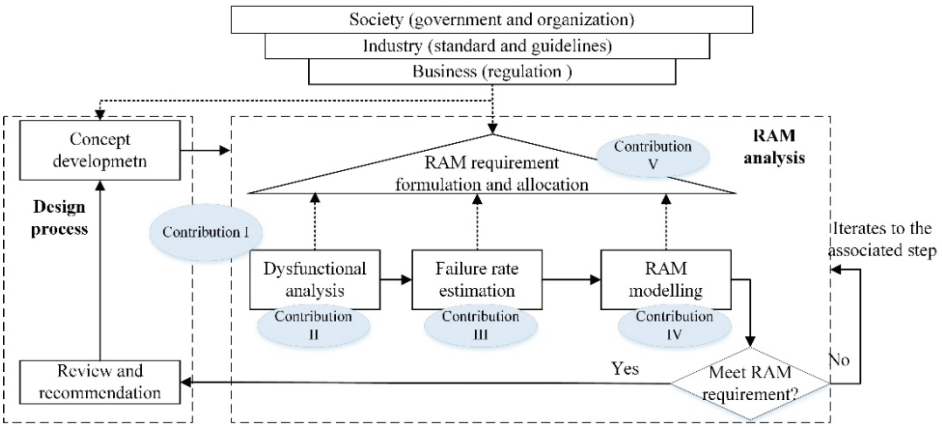


Figure 1-2 Contributions made in this PhD project

The development of new models and frameworks is supported by a closed collaboration with Norway-based O&G industry. The collaborations are in form of reference meeting held semiannually to give inputs and feedbacks for intermediate results, as well as individual meetings (online meeting and visiting to local office). The brief journal of meetings is reported in Table 1-2.

Table 1-2 Mini-abstract per meeting

Date	Description
03/09/2015	• Startups of SUBPRO • Introduction to subproject 3.2
03/02/2016	• Presentation and decisions on status and gaps analysis • Confirmation of main research interests made on basis of literature review and status and gap analysis
17/02/2016	• Theme meeting for future subsea development held in ABB, Oslo
20/09/2016	• Decisions on collaboration with subproject 1.1 • Confirmation on the scientific foundation of new framework development - systems engineering (Aker solution)
27/10/2016	• Theme meeting for subsea reliability held in Høgskolen, Bergen
15/02/2017	• Discussions about contribution I and II
20/09/2017	• Decisions on use cases for contribution I – subsea fiscal metering system (provided by Equinor) • Discussions about contribution III, IV, V
19/01/2018	• Presentation of contribution I to experts in Equinor by visiting the local office in Trondheim • Discussions about potential improvement and possibility for technology transfer
28/02/2018	• Discussions about contribution III • Discussions about the result of this PhD work can be integrated into existing practice and further extension
15/03/2018	• Presentation of contribution III to experts in DNV-GL via skype • Discussions about potential improvement and possibility for further collaboration (interlinked with subproject 3.1)

The thesis consists of two parts as illustrated in Figure 1-3. Part I synthesizes the literature review, and formulates the problem to be solved in this thesis. Chapter 2 briefly introduces subsea technologies and system, and proceeds to identify the related standards and regulations. In the end, a new subsea design

named Subsea Gate Box as the case system is introduced in details. Readers who are familiar with the subsea system may skip this chapter or some sections. Chapter 3 investigates novelty and complexity of new subsea design and study their implications on RAM analysis. 0identifies the scope of RAM analysis in early phase of subsea design, and proceeds to define gaps in existing practice when having a complex and novel subsea system as a study case, as a continuation of the preceding Chapter 3 .

Part II is made of the main works and achievements to this research work, in form of papers published or prepared and some reflections during this PhD project. Five contributions illustrated in Figure 1-2 are presented orderly from chapter 5 to chapter 9. Chapter 5, 6 and 7 are characterized as methodological contributions as the new framework and models are proposed to get rid of identified limits. Chapter 8 and 9 contain discussions and reflections on basis of review work instead. 0presents the summary of all contributions and future works. Finally, this thesis ends with appendices that consists of abbreviations, as well as articles presented in chronological order.

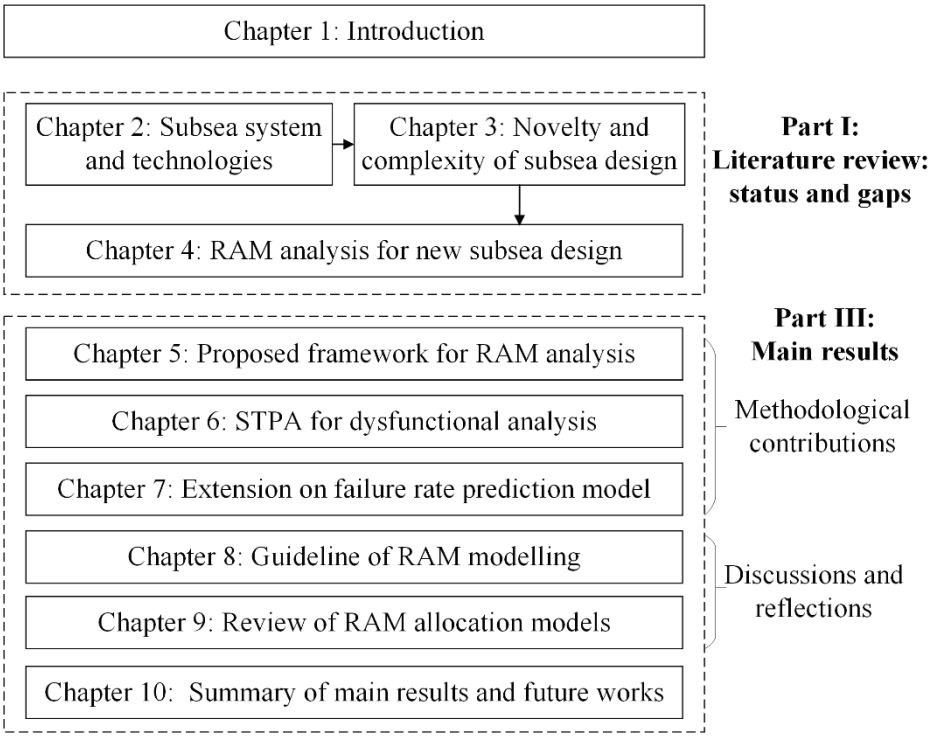


Figure 1-3 Outline of thesis structure

PART I: STATUS & GAPS

Chapter 2 Subsea systems and technologies

About 80% of world's energy consumption relies on fossil fuels including oil, natural gas and coal [23]. The production of oil and gas will continue to be of great importance to maintain the stability of today's energy supply and drive the world's economy, since the technology, availability and transmission of new energy resource (e.g. wind power, ocean power and solar power) have not been fully exploited and approved yet. Such demand on energy consumption drives the development of novel subsea technology, which is key enable for O&G industry in the near future.

This chapter introduces the state of art for subsea system, including key technologies, important frameworks and design considerations when developing products for subsea applications. This begins with a brief description of systems approved subsea or to be placed on seabed. The existing framework used for subsea design is introduced afterwards, followed by the main issues and/or considerations for existing and future prospects of subsea developments are summarized. The overall perspective focuses on issues associated with systems being placed in a subsea operating environment (i.e. from being underwater) and related effects (i.e. high cost impact of intervention and equipment replacement). Finally, a novel concept of field architecture proposed by SUBPRO is presented, to have a practical case for the research in this thesis. The discussions among this topic have been built on existing technical reports from industry [1, 4, 6] and relevant papers and standards [16, 17, 23-29], in addition to presentations and internal seminars given by industry partners in various workshops associated with SUBPRO.

2.1 Overview of subsea systems

The term *subsea* is used in at least two large industrial application areas, O&G and mining. In the O&G sector, which has been the main focus of SFI SUBPRO, subsea technology refers to the exploration, drilling, production and processing of oil and gas in deep waters (often refers to more than 1500 meters in depth). The subsea O&G field development in North Sea was symbolized by the production system in the Ekofisk field in 1971, and has been increasingly matured during the last 40 years by the leading actors in O&G industry [23]. With respect to current marketing situation, increasing operational cost and changing field conditions, it has been a willing to develop a *full* subsea production and processing [1]. It can save the costs in light of manned operation, and increase income by maximizing the recovery rate and extending the life of brown field [6].

The rest of this section briefly depicts three main categories for subsea O&G systems: system production, subsea processing and subsea control.

2.1.1 Subsea production system

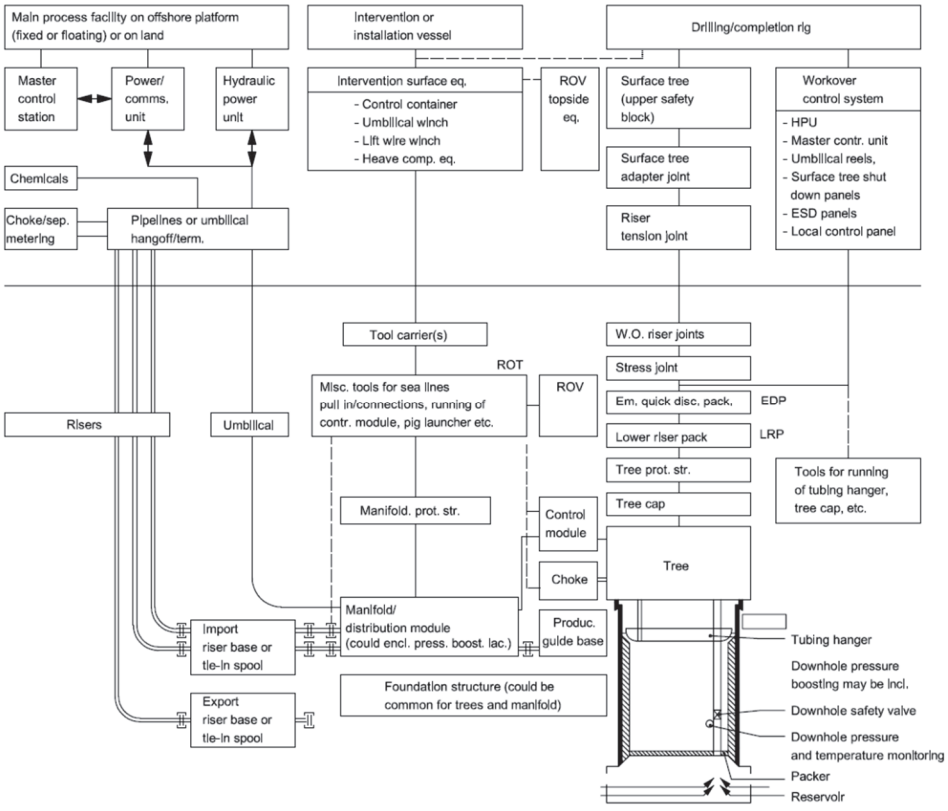


Figure 2-1 Subsea production system, adopted from ISO 13628-1 [17]

Figure 2-1 presents the overview of a subsea production system, which consists of following main equipment to meet the needs of drilling, field developments and field operation [23]:

- **Subsea manifold:** It is an arrangement of pipes and valves installed on the seabed and connected to an array of wells. It is used to combine the flow from different wells and distribute to other facilities/inject water or gas into wells.

- **Wellhead systems:** It is located on the surface of a well as the primary pressure barrier, and provides interfaces for drilling and completion.

- **X-mas trees**: It is a system mounted where the well exits and include several valves to control the flow out from well. The valves can be operated in favor of Remotely Operated Vehicle (ROV) or through the signals from control modules.

- **Umbilical**: It is to link the surface equipment to subsea production equipment, by transmitting the hydraulic and electrical controls, heat, power and chemical injection fluid.

- **Flow line system:** It is made of (flexible or rigid) pipelines to transport oil and lift the gas to surface facilities.

- **Workover system:** It is the system to facilitate the installation, completion, diagnostics, maintenance and repairs.

There are several common configurations of subsea production system and each has a number of variations in equipment, depending on environment of field and operating strategies [17, 23].

- **Satellite wells configuration:** It refers to a single well tied back directly to the host facilities or platforms. This configuration offers high flexibility in installation and operation and optimization of production as each well is handled singly. The potential drawback is the increased cost for mobilizations and the increased number of connections and pipes that implies more points to failure.

- **Clustered wells configuration:** It refers to a group of single wells (preferably placed in proximity) and tied back to manifold that conveys stream to receiving facility. This configuration allows sharing some common functional modules (e.g. flow-line) among clustered wells, thus offers lower costs of field development. The manifold consists of valves and branched pipes to allow operation of different wells. It can be installed also in template described subsequently. The main challenge with clustered configuration is that the intervention on single well of cluster may interrupt the production of other wells as they share some common facilities.

- **Template configuration:** It refers to a large steel structure that provides protective framing and covers for various subsea structures including wells and manifolds. The protective framing and covers are used to reduce the potential interruption caused by fishing activities and other objects. The template is tied back to a host facility.

2.1.2 Subsea processing system

Subsea processing system consists of separation, boosting of fluid, gas compression and treatment, re-injection of water and chemicals, solid management and heat exchanging. The typical equipment for subsea processing are illustrated in Figure 2-2. The structure of subsea processing system mainly depends on the operating strategies, well conditions and distance to receiving facilities. For example, subsea boosting is required in the ultra-deep water and remote field to provide the needed pressure to transport the hydrocarbon to the surface facilities. Existing fields as well as future prospects will require more subsea processing on the seabed, in order to save cost for topside processing and improve flow assurance performance [1, 30]. In this respect, subsea processing system draw more attention in this thesis and is related to the concept of Subsea Gate Box introduced later in section 2.3.

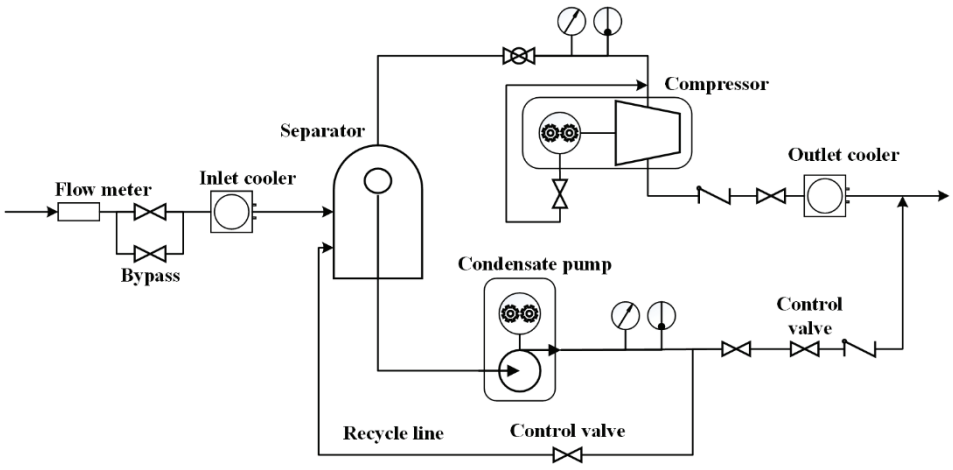


Figure 2-2 A simplified schematic of a subsea processing system

- **Subsea separation:**

The main function of subsea separation unit is to separate the phases (water, oil and gas) of hydrocarbons from wells at seabed facility. This technology can be used in brown field where the increasing water production hinder the recovery of reservoir, or can be applied in green field to reduce hydrate formation thus

reduce the pipeline blockage. Separation technology can be of two types: two-phase (i.e. gas-liquid) and three-phase (i.e. gas-oil-water). The selection of technology depends on water depth, distance from host facility, fraction of water/gas and existence of oil and other product specific parameters. Subsea separation is often used in combination with subsea boosting and subsea compression, such as Statoil's Tordis. Gas-liquid separation contributes to increase the efficiency of subsequent boosting stage.

- **Subsea (liquid) boosting:**

Subsea boosting is sometimes introduced when the pressure declines in the natural reservoirs. Boosting equipment for liquids can be single phase or two phase pumps that are able to transport at the required rate to the receiving facility. In some applications, it can also be used to re-inject the seawater and produced water into well to maintain the pressure of reservoir thus increase production rates. Subsea boosting has potential to accelerate the production or enable the production of low energy wells. Subsea boosting of water, oil or multiphase fluid may be the most mature technology in subsea processing. Depends on differential pressure and gas volume fraction, subsea liquid boosting can be categorized as: multiphase pump, single phase pump and hybrid pump [31]. The available pump technologies are separated into two categories: positive displacement pump and rotodynamic pump. The former category includes twin-screw pump, and the later include helico-axial pump and centrifugal pump.

- **Subsea (gas) compression**:

Subsea compressors may be introduced for the same purpose as for liquid boosting, but for handling of gas fluids. In general, subsea gas compression is not at the same maturity level as subsea boosting and subsea separation and there exists only three solutions [32]. The compression technology can be separated into two categories: dry gas compression and wet gas compression. The dry gas compression relies on capacity of gas-liquid separation. The existing solutions are Ormen Lange subsea compression pilot and Åsgard dry gas compression (similar design with Ormen Lange). The wet gas compression can handle the water fraction up to 20%. The existing solution is the wet gas compression installed in Gullfaks.

2.1.3 Subsea control system

Subsea control systems provide controls to remotely operate on/off valves, control/choke valves, Xmas trees and other actuators on the subsea production and processing systems, based on transmitted data and signals received between surface and seabed.

The subsea control system consists of two parts. The first part includes the equipment installed in *topside*, such as electrical power unit (EPU), hydraulic power unit (HPU) and associated junction box. The second part includes equipment installed *subsea*, which consists of umbilical, umbilical termination unit, subsea control module (SCM) and the like.

Depending on the type of interfacing equipment, distance and number of connected subsea equipment, there are five technologies available for subsea controls [23]:

- Direct hydraulic
- Piloted hydraulic
- Sequenced hydraulic
- Multiplex electrohydraulic
- All-electric

Hydraulics have been the traditional medium involved in the control of subsea valves. There are two main design concepts: direct hydraulic control and electron/hydraulic control. The direct hydraulic control system requires few subsea component, where valve is controlled by individual hydraulic line from HPU installed topside. The piloted hydraulic control system requires the use of SCM. When the command is sent to open the valve, the pilot valve mounted on SCM opens to allow the hydraulic fluid flow into the tree valve. The operation of sequenced hydraulic control system is the same as the piloted hydraulic control system, but the sequence of operating valves is taken into account thus it is more feasible to handle complex control operation. In general, from direct hydraulic control to sequenced hydraulic control, the response time and the distance of tiebacks increase.

The multiplex electrohydraulic control system has replaced hydraulic control system in most subsea developments, by adding electronics on subsea electronic module (SEM) and master control station (MCS). The overview of multiplex electrohydraulic control system is shown in Figure 2-3. When there is a demand to operate the valve on trees, the human operator sends the coded command from MCS to SEM through umbilical. SEM can distribute the control command to associated valve that is energized or de-energized by the hydraulic fluid. The sensors or meters connected to SEU allows monitoring the technical states of process and production equipment. Subsea distribution unit (SDU) can distribute commands to other subsea systems or modules, where the connection is made of inter-module cabling, e.g. jumpers.

The next generation of subsea control is the all-electric control system. The electrification of control system has many benefits such as the faster response from command to operation, increased flexibility for self-diagnostics and monitoring, and less potential pollution by eliminating the hydraulic feeding in umbilical line (i.e. the blue line in Figure 2-3). Nevertheless, there are new challenges and barriers to overcome before all-electric control system can be fully used for field development. For instance, the increasing number of connectors and the electric hardware system and the intensive use of electric software system both implies the severe impact on system reliability. Well proven reliability of new product, well-documented technology feasibility and costs for complexity, production downtime, manufacturing and documentation are all needed to demonstrate such new design is a better solution.

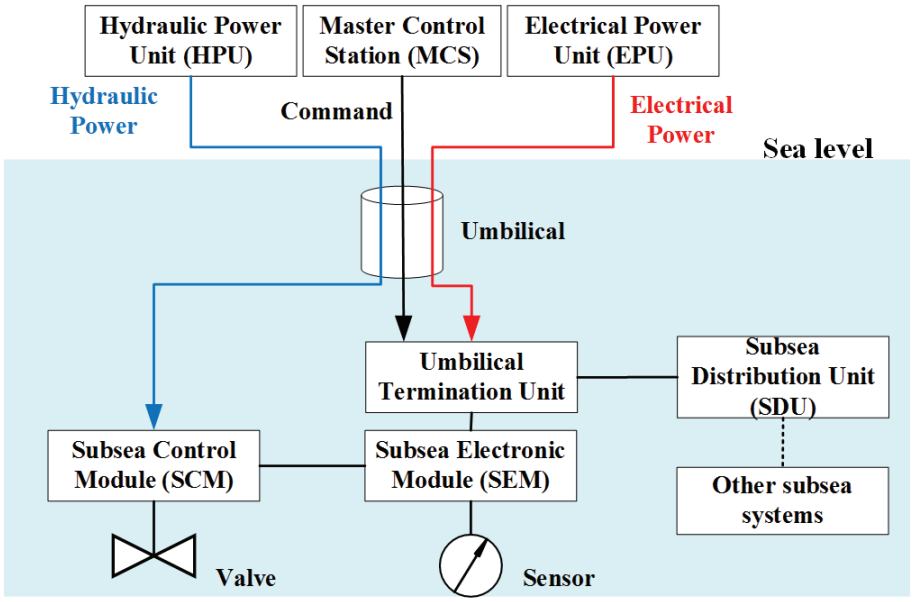


Figure 2-3 A simplified schematic for multiplex electrohydraulic control system

2.2 Frameworks for subsea design

Most manufacturers and system integrators of subsea technologies have internal design procedures and practices. They are developed on basis of regulatory requirements and recognized national and international standards. In addition, they may address other considerations, such as delivery targets (e.g. client specification in contract), technology feasibility, and resource (e.g. budget and timing issues of production realization).

Of regulatory requirements, it is important to consider clauses in Petroleum Safety Authority (PSA) that concerns Norwegian continental shelf. PSA regulation[1] provides a complete collection of high-level needs, which may be considered based on the relevance of specific system or design alternatives. For instance, the following clauses may be applied in general for a new subsea design:

- Framework regulation §45 Development concepts
- Framework regulation §48 Duty to monitor and record data from the external environment
- Facility regulations §9 Qualification and use of new technology and new methods
- Facility regulations §10 Installations, systems and equipment
- Facility regulation §12 Materials
- Facility regulation §34 Process safety systems
- Facility regulation §55 Production facility
- Activity regulation §50 Special requirements for technical condition monitoring of structures, maritime systems and pipeline systems

There are also many standards of relevance to subsea systems. For technical standards that regard design and operation, some of example standards are:

- Subsea production systems: ISO 13628-1 [17] (alternatively API-RP-17A [26]) and NORSOK U-001 [18]
- Processing system: NORSOK P-001 and NORSOK P-001 [33][2]
- Subsea production control system: API-17F [34]
- Drilling facilities: NORSOK D-001 [35]

For RAM-related standards, some standards are commonly referenced:

[1] PSA website: http://www.ptil.no/regulations/category873.html
[2]This is based on topside requirements, and there is no subsea version.

- Risk and reliability associated with production assurance: ISO 20815 [14] and NORSOK Z-013 [36]

- Reliability data collection: ISO 14224 [37]

- Reliability modelling and calculation: ISO/TR 12489 [9]

- Technology qualification: DNV-RP-A203 [15] and API-RP-17N [16]

In addition, for functional safety of subsea systems, the main reference is NOG-070 [38] issued by Norwegian Oil and Gas Association, which is based on the generic standard IEC 61508 [39] and its specific version for process industry-IEC 61511 [40].

The existing framework from generic standards like IEC 60300 [10] also provides rigorous steps and associated models to predict, review and improve RAM performance of a system. These frameworks do not have any real shortcoming but they may present a few inadequacies regarding applicability for subsea system. For instance, the generic standards may not (and they should not) give higher awareness to subsea specific considerations and constraints of early design phase, thus the approach is often taken without necessary justifications and explanatory comments. Moreover, the standards and requirements for subsea design have grown organically with market situation. They may be ambiguous and open to large degree of interpretation. This may cause that extensive time may be spend on requirements that have few or no impact on the quality of end product.

2.3 An example of a novel design concept: The subsea gate box

A review of trends and prospects for future and full subsea development includes (but are not limited to) the following findings [4, 28, 41]:

- **Configuration and architecture of subsea systems**: The more compact and modular architecture is required for flexible operation and maintenance in subsea context. The light weight and reduced footprint are also required to facilitate the installation and intervention of subsea systems.

- **IMR strategies for remote subsea fields**: Some subsea equipment may be designed not be replaced until intervention. They are exposed to obsolescence issues, thus the needs of monitoring technical states are

increased accordingly. In addition, the cost of replacement and intervention for equipment placed on seabed is drastically increased.

- **Lifetime of subsea equipment in the harsh environment**: Future subsea development may move toward a hostile environment characterized by deep water (up to 3000 meters), extreme temperature (ranges from -50 °F to 350 °F) and high pressure (up to 15000 psi). This leads to flow assurance issues like hydrate formation, wax deposition and increasing pressure drops.

- **Autonomous/unmanned process control**: For long distance tied backs, there is no sufficient time for operation reaction in demanding/emergency situations. Automatic controls therefore become needed and it has significant benefits for both operation safety and economic. To increase the response time, the need of programmed functionalities and the dependence on computer control are largely increased.

In together with current market situation, it has become clear that O&G industry needs to develop new solutions where possible to reduce costs and increase production [6]. Hereafter the term *new subsea design* refers to the design incorporates aforementioned considerations without compromising on safety and environmental protection. Subsea Gate Box (SGB) developed by subproject 1.1 of SUBPRO, is considered as a representative for new subsea design.

So far, the development of SGB is at conceptual design stage, where many details have not been decided yet. In the first three years of SUBPRO, the progressive focus of subproject 1.1 has concentrated on the technological assessment and feasibility study of configuration alternatives of SGB.

SGB is a modular and multi-functional assembly that enables dedicated processing solutions to prepare hydrocarbon stream from a single well, or satellite wells or the cluster of wells, before it is transported to the receiving facility like manifold. The architecture of SGB follows LEGO principle as shown Figure 2-4, where the proper subsea processing equipment are selected to meet different separation and boosting needs. In addition, SGB consists of corresponding equipment for processing according to the necessity of the wells, e.g. flow meters, choke valve, utilities for control and instrument, and associated connections and umbilical. The functional units located on subsea modules act independently to perform the specific task under normal operation, or together in synchronization to be replaced or restored upon abnormal situation. Considers SGB#2 in Figure 2-4 as example. The resource of hydrocarbon can be wells or other nearby SGBs. In the normal operation mode, hydrocarbon flow into separation module and be

separated as liquid and gas (or oil, water and gas if three-phase separator is used). Then the hydrocarbon flows into pipeline with metering station so the flow rate for gas and liquid can be determined and the sample of hydrocarbon can be extracted if necessary. The liquid can be boosted via selected pump thus transported to manifold, where the gas is assumed to flow naturally. When boosting module or separation module are not able to carry out defined functions, they are isolated by closing valves and hydrocarbon is bypassed to the choke module, where the choke valve controls the pressure of hydrocarbon thus enable transportation. In such temporary arrangement of SGB, the efficiency is reduced due to the inadequate subsea processing for hydrocarbon.

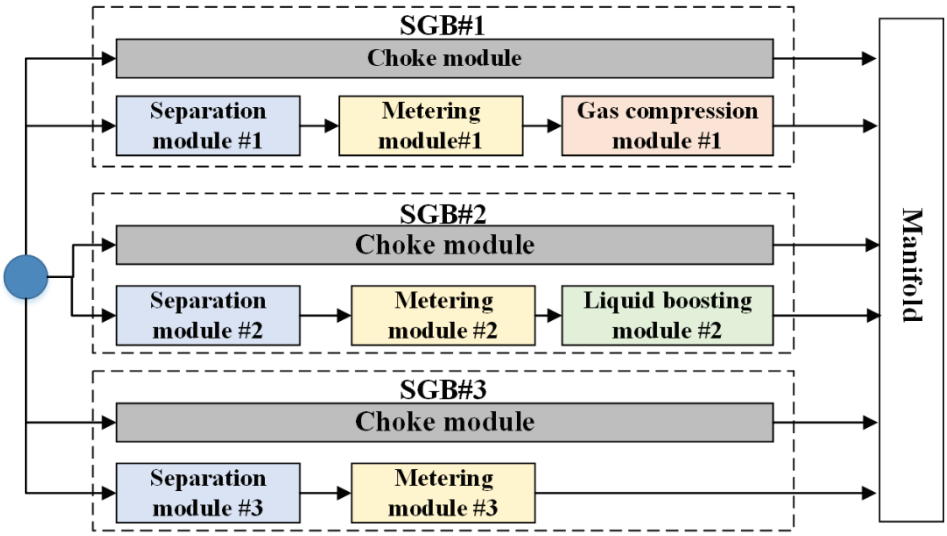


Figure 2-4 The illustration for typical SGB architecture

The main drivers for SGB are summarized as following [28, 32]:

- The overall performance of field is optimized by SGB, in terms of increased recovery rate and accelerated production.
- The functional modules are customized according to constraints posed by different wells and the changes in recovery strategy, which increases the operational and control flexibility. The modular design minimizes the use of processing equipment and allows the future modifications and extensions in the field without compromising (e.g. add-in assembly and tie-back development), which results in the reduction of capital expenditure (CAPEX).
- The commingled fluid of different wells streams is avoided as the dependences between resources of hydrocarbon in the network are

removed. The high modularity of SGB facilities the operation IMR, which reduces operational expenditure (OPEX).

Meanwhile, several challenges are introduced by SGB. First, there are some technology gaps for SGB, for example the related technology for compact separation has not yet qualified for subsea application, which implies a considerable effort to reduce technical uncertainties before putting into operation. Second, improving the operational flexibility of SGB results in an increase on the number and diversity of equipment, which implies an increase on weight/footprint. This gives challenges for integrating it into existing well or manifold design solution and determines the major elements in life cycle cost of SGB as a higher capacity vessel is required.

In this respect, the main concern of SGB design is relative to reliability that incorporates the downtime and availability incorporates effects of maintenance and operations. RAM analysis is therefore required to support the major *decisions* in maturing the concept of SGB. The decisions involve suggesting countermeasures and design modifications (e.g. redundancy and safety barriers), and selecting different alternatives of system architecture and IMR strategies.

Chapter 3 Novelty and complexity of subsea design

The continued reservoir development in a mature or marginal fields is made possible by new subsea designs. There are two main aspects for new subsea design, namely *novelty* and *complexity*, which imply (negative) implications or constraints for RAM analysis.

This chapter is therefore divided into two parts. The first part is to clarify the notion of novelty, and study its impacts from industry perspective. The second part is to investigate the meaning of complexity from academic side and characterize it for subsea system.

3.1 Novelty of new subsea design

A new subsea design represents the advance in technologies and innovative improvements as the solution to future subsea development. Meanwhile, it is often met with skepticism as a high level of novelty is always introduced. This section addresses the following questions in related to the novelty of new subsea design:

- What aspects/parts of a new subsea design signify the novelty?
- What are issues/challenges to be addressed in RAM analysis, given the novelty of a new subsea design?

3.1.1 Degree of novelty

Most of novel subsea design is not from scratch. They are based on comparatively old and stable technology transferred from topside (platform-based) exploitations to have novel concepts for subsea operation. Still, a new subsea design may have a high degree of novelty associated with the need to implement new technologies and ways of operating. This requires attempts to qualify the new technology in a throughout process to achieve its intended gains. Such process is called technology qualification program (TQP) to prove that the new technology functions reliably with an acceptable level of confidence [15]. RAM analysis therefore plays an essential role in a TQP, in charge of specifying how the system shall detect and respond to failures, how the system performance can be demonstrated prior to installation, and how the system can maintain its performance under changing operating environment.

In O&G industry, DNV-RP-A203 [15] and API-RP-17N [16] are two recommended practices for TQP. Both of them have individual approach for acknowledging the notion of novelty. API-RP-17N [16] adopts the concept of

technology readiness levels (TRLs) that is firstly developed by NASA [42]. TRL is a measure of maturity in the qualification, and builds on evidence from qualification activities, such as the passing of specific milestones in a TQP [15]. Rather than using evidence-based measures, DNV-RP-A203 [15] proposes a more concise and comprehensive way to acknowledge the degree of novelty. As reported in Table 3-1, there are two dimensions for signifying novelty. One is the technology itself (e.g. parts of a large system) and another is its application area (e.g. operating conditions and environment). A system is considered as 'proven and known' when it belongs to category 1. No technical uncertainty is attached with category 1, meaning that RAM performance can be assessed by existing standards. A system is considered as 'novel' when it falls into category 2, 3 and 4, with increasing criticality for qualification task.

Table 3-1 The categorization of novel technology, adopted from [15]

	Technology level		
Application area	Proven	Limited field history	New or unproven
Known	1	2	3
Limited Knowledge	2	3	4
New	3	4	4

Here considers subsea liquid boosting system as example. Electrical submersible pump (ESP) is considered as a viable technical solution for subsea boosting [43]. The most experienced application of ESP is on the downhole environment, where it is placed on the vertical position and designed to be long and slender to maximum the lift of pump due to the relatively small-bore casing. For subsea boosting purpose, one feasible design concept is to place ESP on the horizontal section of a flow line jumper that is used to connect subsea units. It favors maintenance and has minimal impact on existing subsea structure when installation, since the deployment of ESP assembly is the same as is done for a flow line jumper [44]. In this regard, subsea boosting with ESP technology may belong to category 2 or more likely 3 due to significant changes in application area (i.e. from downhole to subsea) and it is assembled in a different way (i.e. from vertical position to horizontal positions). By contrast, the sensors installed on boosting equipment may belong to category 1, or 2 if some modifications are made based on new needs of inspection and condition-monitoring, e.g. computer-based measurement for quick localization of faults.

One notable aspect is that Table 3-1 is not used to indicate RAM performance of a system, as it does not consider the effect or consequence of failure. For instance, a system with category 4 represents the highest technical uncertainty, but its failure may not represent the greatest impact on system performance. Instead, the degree of novelty is to indicate the *efforts* (i.e. the aspects be addressed) of RAM analysis, which is discussed in the following subsection.

3.1.2 Challenges with subsea novelty

Guided by a twofold perspective in Table 3-1, this subsection is decomposed into following point two points[3]:

- **The conservative design compensated for unknowns in technology**

The new market situation for O&G industry requires that subsea systems are built with a sufficient level of reliability and availability at a cost that is less than today. The RAM requirement may be much stricter than topside for the same technology or systems, to reduce the possibility of economical consequence subsea such as costly interventions. Changes may relate to new hardware and software that meet subsea reliability requirements, which in turn leads to *unknowns* in design and operation. For instance, the increased dependence on computer controls may result in some unfamiliar hazards caused by flawed specification and software errors, which may not be easily revealed. Changes may also relate to new architecture, configuration and system interfaces. The *unknowns* may lead engineers to choose a conservative design with a higher level of redundancy and demanding safety requirement, which in turn implies more cost than expected. The investment in redundancy for optimizing the production is not always profitable as it may achieve very little overall the system availability. For instance, more interconnections for communication between the redundancy and the main system (e.g. valves and jumpers) represent more points to failure thus RAM performance is compromised, and they are both exposed to same environment so common cause failure (CCF) is expected. As extra time and cost must be spent on fulfilling too high reliability target subsea, it becomes more difficult to demonstrate that moving from topside to subsea is a smart idea.

Resolving this challenge requires not only the effort to establish the confidence for new technology, but also an early trade-off between '*essential*' and '*nice to*

[3] The main content here has been derived from comments and feedback from in-kind report by Aker Solutions and workshops held by ABB on 17th February 2016, in addition to presentations given by industry partners in various workshops associated with SUBPRO.

have'. It is more important to identify a *best* performance considering the constraints of operation and environment, rather than the theoretically *optimal* performance. To achieve this, a more systemic view in RAM analysis is required, in order to reduce the category of unknowns and costs paid for conservativeness.

- **The exposure to subsea environment**

Even though a system characterized as 'subsea' means it is placed underwater, the application area of subsea systems may vary. A certain amount of novelty is introduced by limited experience of operating conditions (e.g. high temperature and high pressure reservoirs or field with high CO_2 content) or environment (e.g. arctic seas).

The major influence of exposing to challenging application areas is on the degradation of subsea equipment. This implies an increase on: (1) the failure rate of subsea equipment if no preventative maintenance is carried out subsea; or (2) the need of condition based maintenance or other soft means for isolating the faulty equipment to continue required function (e.g. processing of petroleum products). Resolving the first issue relies on a comprehensive identification of factors that influence the failure rate, to be named reliability influencing factors (RIFs). The evaluation of RIFs in different application areas is therefore critical for assessing RAM performance of new subsea design. The second issue calls for a willingness to accept degraded operation over time. The overall (production) performance can settle on different levels depending on states of a system. This means that multi-state and multi-unit system is generally assumed for RAM modelling and it can be complicated by dependencies between system and its parts. For example, a system may be reconfigured in presence of failures on one or a set of parts. Such dependencies in structure can hardly captured by static modelling, which requires the use of dynamic modelling driven by simulation tools.

3.2 Complexity of new subsea design

Many research works are attached with the term *complexity*, to indicate the difficulty of problem or incomprehensibility of system being studied [45]. Despite a large body of literature on complexity-related topics, it is always a challenge to position the concept of complexity in RAM analysis and investigate its impact on produced models and used concept. This section addresses the following questions in related to the complexity of new subsea design:

- What is the meaning of complexity in the context of RAM analysis?

- What aspects/parts of a new subsea design contribute to characteristics of complexity?

3.2.1 Concept, definition and interpretation of complexity

The term *complexity* and its adjacent form *complex* are frequently used in our daily expressions, mainly refers to the state that being intricate. This term is used slightly differently in science and engineering discipline. It is to characterize the nature of an *object* and indicate the difficulty in describing and understanding it. In this thesis, the notion of *system complexity* is preferred to distinguish from the daily use.

A precise understanding of system complexity is to identify the limitation of analysis and determine the confidence of associated results. For an engineering design problem, underestimating system complexity may lead to false comfort that the system is well designed, meaning that analysts fail to anticipate potential design error and under the risk of costly re-design [46]. Similarly, overestimating system complexity means that countermeasures for weak points are not properly recognized in analysis, which may lead to pessimism in design.

The definition of system complexity could be discipline-specific, depends on the object of study and assessment context. For instance, complexity defined by computer science is essentially different from complexity defined from perspective of social science. In this thesis, the system complexity is defined upon the engineering system being analyzed in RAM analysis, which is influenced by its way of design (including its construction) and its way of being operated (including maintenance). A system defined as complex by RAM analysis may possess few of complexity characteristics defined by complexity science/theory [47-49]. For instance, one complexity characteristic is *self-organization*, means that a system attains the current structure without external interfaces (e.g. central director in controls) [50]. The example systems can be traffic, stock and securities market and global climate change, where each entity on the complex system *adapts* itself flexibly according to surrounding environment and/or manipulates the externals. Most of engineering systems does not have such attribute, because such emergent behavior without central controls can hardly be designed or engineered. The related discussion also touches the concept of resilience engineering [51], which is obviously beyond the scope of this thesis.

To continue the discussion it has to pay attention on a previous generalization of theory, that is normal accident theory (NAT) proposed by Perrow [52]. NAT emphasizes that the concept of complexity lies in *interaction* of a system: '*those of unfamiliar sequences, or unplanned and expected sequences, and either not*

visible or not immediately comprehensible'. The accidents or other types of loss are *normal* (to happen) when interventions on complex system is limited or largely constrained. One notable point is that NAT focuses on the concept of *interactive complexity* or *complex interactiveness* rather than complexity itself [53].

Two counter-concepts are therefore introduced: *complicated system* and *linear interaction*. A complicated system may be difficult to understand or incomprehensible, as it consists of numerous entities and/or associated connections. Once sufficient time is spent on gathering knowledge about entities and/or associated connections, the behavior of a complicated system is rather predictable and readily analyzed. This means that unlike novelty complexity cannot be reduced by gaining knowledge and experience, that is called as *incompressibility* of complexity [50]. In contrast to complex interactions, linear interaction is expected or visible even if unplanned. It should be noted that most systems are subject to linear interactions, but a linear system can still occasionally own complex interactions, as a result of being operated under specific environment. In this sense, complex system may not be simply seen as opposite of linear system.

In my view, Perrow's contribution on complexity is mainly with respect to *ontological aspect*. System complexity is then interpreted as an inherent property of a system: a system possesses many parts and they are interacted in various ways that are not easy to comprehend, can be seen as complex. This relates to the nature of a system itself in form of its construction, the way of operation and maintenance and its interaction with environment. The next section is to identify main characteristics of a complex system, where SGB is used as an illustrative case.

3.2.2 Characteristics of a complex system

A system can signify many different elements. Figure 3-1 illustrates a general idea of *socio-technical* system, where *socio* refers to human and organizational factors (e.g. standards, enterprise management, project management, operation and maintenance management) and *technical* refers to hardware and software factors including their physical structure and implementing technology. The complexity of socio-technical system arises from interactions between social factors and technical factors, represented by dashed line in Figure 3-1, which may increase or decrease (RAM) performance by providing good services or implies more hazards when bad practice. For this point of view, the more factors recognized to be a system, the higher the complexity. After discussion with industry partners, this thesis is mainly restricted on technical side, thus the

boundary of subsea system is agreed on hardware and software component and their interactions to operation and maintenance.

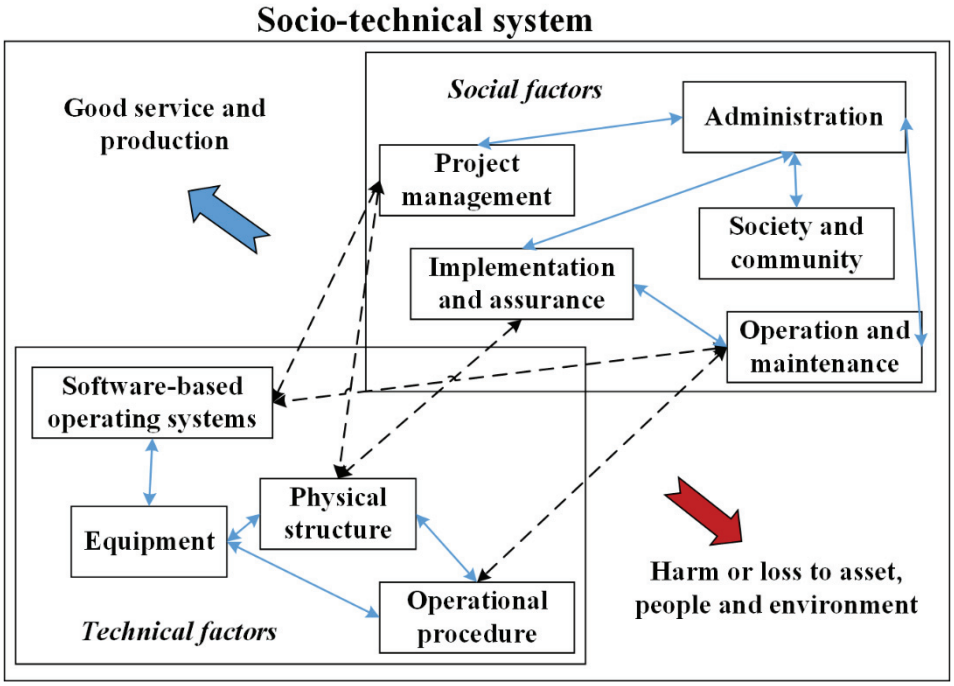


Figure 3-1 A illustration for socio-technical system, modified on basis of [54]

In this context, the general characteristics proposed by Perrow [52] can be used to acknowledge system complexity. Few of them are self-explaining, thus some interpretations and explanations are added as following:

- ***Tight spacing* of equipment:** this refers to the geographical closeness between system parts, which can result in unexpected behavior of system from failure propagation (cascading effects) or common (excessive) exposures.

- ***Proximate* production steps:** this refers to the lack of independence between separate phases of production. This means that the production is tightly coupled and non-sequential, saying that parts tend to be functional dependent. The implication is the major disturbance or adjustments on production sequence (e.g. temporary shutdown) during maintenance and repair activities.

- ***Common-mode connections*** **of component outside production sequence:** this refers to unexpected behavior of several system parts, caused by the sharing or reliance on external components, such as power supply.

- **Limited *isolation* of failed components:** this refers to the limited easiness and timeliness to pull out or remove failed parts. This means the lack of spatial segregation between parts, which implies the physical dependence. The isolation of failed part therefore result in the disturbance on the rest of system, such as removal of other parts to get access or re-configuration.

- **Personnel specialization limits *awareness of interdependences*:** this refers to the situation that specialized personnel may unexpectedly interact with system under special circumstances. Conversely, the generalists (who know basic of other's role and duty) are more likely to diagnose the unexpected interactions and more likely to cope with them, which impedes the escalation from incidents/errors/mistakes to system level accidents.

- **Limited *substitution of supplies and materials*:** this refers to highly specialized requirements (i.e. 'less standardization' as engineers call it) of components. Therefore, a complex system has less substitutability, which limits the potential to replace the faulty component.

- **Many *control parameter* with potential interactions:** this refers to the potentially unexpected behavior of the system from interacting with controllers. Today's engineering systems often require a higher level of automated controls for intelligent, adaptive, and fast response in operation, such as subsea systems installed remotely. For complex system, control parameters can be less direct and segregated, thus resulting in unintended interactions that may contribute to loss of functionality.

- **Unfamiliar or unintended *feedback loops*:** this refers to the situation that system designers fail to anticipate all the possible inputs to controller (e.g. the possible operational and emergency scenarios). The controller may be puzzled by unfamiliar context, thus it is more likely to signal the unwanted control commands. The use of multiple controllers may amplify the situation, since the interfaces between

controllers could be extensive. This implies the need to have a complete functional specification of controller at the first place.

- **Indirect or inferential *information sources*:** this refers to the lack of proper means to measure the technical state of equipment in complex system, for example where the sensors are practically impossible to install (e.g. inside the reactor or extreme subsea environment). The controller may rely on other alternative information to predict and indicate the real state of system, where some uncertainties are attached. This may result in missed, misunderstood, or misinterpreted signals in feedback loops thus unexpected interactions are possible.

- **Limited understanding of operation and *transformation processes*:** this mainly relates to biochemical technology, chemical plants and nuclear production. For instance, the transformation of chemical product may not be fully understanding due to the change of environment and production steps. This can be solved by gaining more experience, e.g. experiment and lesson learnt from trial and errors.

The importance of the listed characteristics may have changed over time, due to the changes in technologies used. For instance, the characteristics listed above relate mainly to hardware-based system, since programmed systems where not so widely used when the list was first developed. Some practical considerations can be implemented to complement the list. For instance, time constraints and distributed decision may be included as response to the changing role of software and human in engineering system built today. Still, the list can satisfactorily give a comprehensive understanding of a complex subsea design, if some explanatory examples and comments are given. Table 3-2 specifies the complexity of SGB. Even this specific installation is considered, the specified complexity is relevant for new subsea design in general.

Table 3-2 Factors contributed to complexity of SGB

Complexity characteristics	Specification on SGB
Tight spacing of equipment	The modularization of SGB makes it more integrated and physically compact, to accommodate weight and size constraints of integrating SGB into existing wells or manifold design solution.
Proximate production steps	The subsea processing functions are highly dependent. For instance, the malfunction of separation module may interrupt the subsequent production steps. For instance, when the scrubber is malfunction or work improperly, one possible consequence is liquid level inside the scrubber is too high then it may flow into gas compressor and cause severe damage on rotating pumps.
Limited isolation of failed components	Some components inside SGB cannot be pulled out without lifting the whole structure, e.g. metering modules. Designing countermeasures to prevent failures or enhance robustness (by having redundancy) are relevant considerations.
	In addition, many subsea fields have special restrictions associated with accessibility. It may take several months for mobilizing the vessel to retrieve faulty equipment. As compensation, through the use of redundancy/adding more parts (e.g. bypass choke module), which in turn increase complexity in another way.
Many control parameter with potential interactions	The remote control for SGB is highly automated to enable fast control for the compact process modules. It is also necessary to separate (functionally or logically) the function to isolate the well upon an emergency situation. The controls on subsea system tend to make the component interact in a linear and sequential way. One major challenge is the long distance (normally one kilometer or more) between the controller and component. This situation requires some intermediate controllers in-between, which in turn increase the number of feedback loops and potential interactions.
	Another concern is the extensive use of software. The embedded software can be seen as the source of unreliability. It cannot physically fail due to wear and tear, but it can still contribute to the failure of system.

Indirect or inferential information sources	Monitoring of technical states of equipment on SGB may require additional sensors, which introduces more penetration probes and possibility for sensor failure. Some physical measurements may be replaced by estimation, using a combination of other available measurements and degradation/performance models. Estimation models may add complexity, and also possibility of unexpected (and unrealistic) readings under special conditions.

As reported in Table 3-2, some complexity characteristics may seem difficult to be eliminated, e.g. low possibility of timely fault isolation due to its remote location. Some characteristics may seem to be preferred by designers, e.g. multiple control stations, programmed functionalities, modular and compact design. Being complex does not necessarily implies that the design concept is undesirable. In fact, complex system could be more efficient in terms of more multifunctional components and less tolerance of low quality performance [52]. From this point of view, we *welcome* complexity in new subsea design, meanwhile the effort must be devoted to acknowledge and address complexity in relevant assessment context thus reduce catastrophic potential and prevent loss of production.

The *degree* of complexity can be quantified by assessing the weight or criticality of these characteristics. For present analysis to identify the critical impacts of system complexity in RAM analysis, such quantitative modelling is less important. The readers interested can find a variety of works on this topic, e.g. the dissertation of Sammarco [55] and the work by Johansen and Rausand [45].

Even though a set of complexity characteristics could be defined in the spirit of Perrow [52], their implications may vary given the choice of model, background knowledge bases and associated decision contexts. This naturally raises another question: *whether such process of acknowledging complexity generates any subjective difference between different assessment contexts*? In such context, the inconsistency between disciplines may result in the difficulty of describing and understanding a system concept, that is often denoted as *epistemological aspect* of complexity [45, 53].

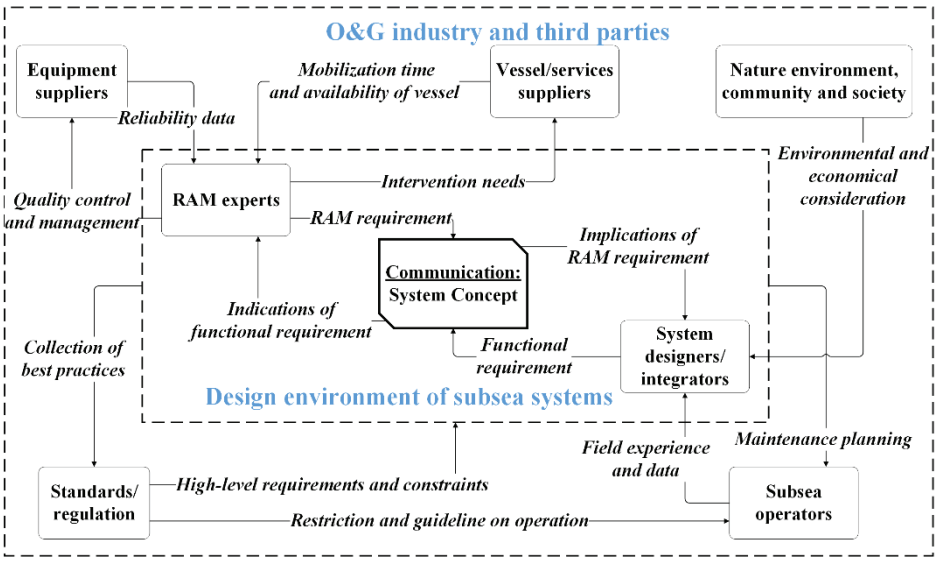


Figure 3-2 Main stakeholders involved in new subsea design

Multiple disciplines may contribute to mature the concept of new subsea design. As specified in the introduction, they are classified into two domains, namely system designers and RAM analysts. They are recognized as primary stakeholders in subsea design process as illustrated in Figure 3-2, where the secondary stakeholders, for example subsea operators, are responsible to support the analysis of two domains. There are often conflicting interests between these two domains, reflected by inconsistency of their models and focus of their elaborations. *System designers* are in charge of developing and maturing technical aspects of design concept by integrating expertise feedbacks from multiple-disciplinary specialists, e.g. chemical, mechanical, and software engineers. In this regard, models developed by system designers, hereafter named as *system models*, focus on the seamless communication between disciplines, which facilitates in understanding how the system can work. The example could be piping and instrumentation diagram (P&ID). It is used to illustrate the physical connections and flow paths, which supports safety and operational investigation later. *RAM analysts* are in charge of assessing system concept based on an error-prone point of view. The ultimate goal of RAM models is to understand how the system may fail upon stated conditions and constraints and obtain associated quantitative indicators. The results of RAM models are primarily used to support decision making about redundancy, modularization, strategies for interventions and the like.

Now returning to the question raised earlier. Although the same system concept is considered from a holistic perspective, understanding system complexity is

conditioned on heterogeneity and discrepancies between domains (more strictly speaking, their produced models). On the one hand, there is no single 'best' model to account for all complexity characteristics. Some characteristics may draw more attention in one domain than the other. Involving models built on multiple perspectives provides more possibilities to mature the design concepts. On the other hand, the frictions between these two domains may restrain communicating system complexity. If the system model cannot be fully comprehended by RAM analysts, the result of RAM models may be questionable or threatened by subjectivity. This is also supported by O'Connor and Kleyner [56] who pointed out that other engineering teams do not easily observe the effect of RAM considerations and accept the associated modifications. If there is a suitable framework to integrate all relevant disciplines into a team effort, involving RAM analysts is more of opportunity than problem to improve the subsea design concept.

In a short summary, this chapter has presented some reflections on novelty and complexity, and discussed how to characterize these two aspects in the context of new subsea design. The next step is naturally to structure them into RAM analysis, find limits of previous generalization, and improve by which new models and frameworks developed in this research project.

Chapter 4 RAM analysis for new subsea design

This chapter is to identify specific research gaps related to the execution of RAM analysis in the early design phase. The starting point is the identification of special considerations for RAM analysis associated with early design phase, considering novelty and complexity of new subsea design. Afterwards, requirements for new models and framework are identified accordingly.

4.1 System development process

The stakeholders of a system have been more aware of its RAM performance, in order to optimize production and reduce risks to human life, property, environment and finance. RAM analysis in this sense serves two main purposes: (1) to raise new issues to consider when developing a system, and (2) to indicate life expectancies and intervention needs thus suggests modifications to a system [57]. This implies the necessity of anchoring RAM analysis in the system development process.

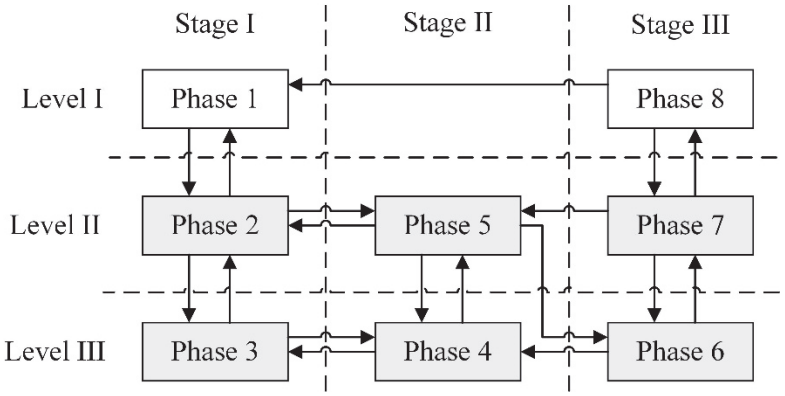


Figure 4-1 System development model, modified from [58]

A system development process consists of several phases and steps, where different models have been proposed and adopted by industry. They are complicated by industrial competition and rapid pace of technology innovation, although they are subjected to great similarities. The system development model proposed by Murthy et al. [58] is commonly adopted in RAM community and so as in this thesis. As shown in Figure 4-1, it demonstrates an iterative process to determine, allocate, and implement the system performance and specification. The product perspective is divided into three levels: business (level I), system (level II) and component (level III). The development process is divided into three stages: pre-development (stage I), development (stage II) and post-development

(stage III). In total, eight life cycle phases for a product have been proposed. They are carried out in series within increased details and own to iterations and review, as indicated by arrows in Figure 4-1. As long as focusing only on the technical aspects, the business level (level I) may be eliminated from analysis so only six phases (colored by grey) draw attention in this research work.

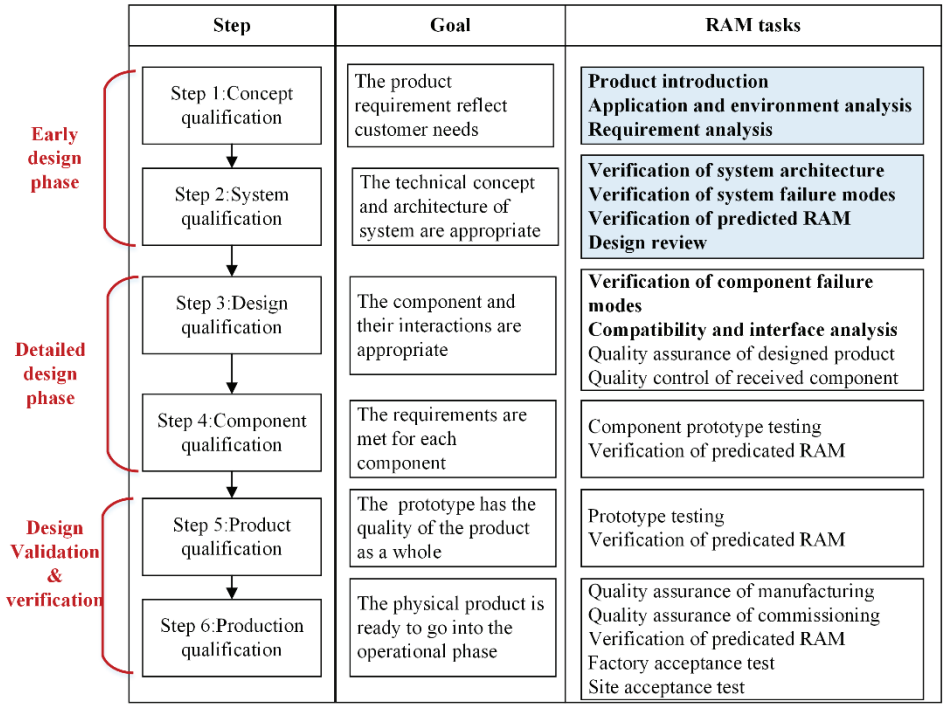


Figure 4-2 An example of TQP framework, modified on basis of [59]

As a continuation of Figure 4-1, Figure 4-2 illustrates a new TQP framework TQP proposed by Rahimi and Rausand [59], where six main steps covering from conceptualization to production are included. The early design phase can be illustrated as step 1 and step 2 in Figure 4-2. Given a set of customer needs (in terms of operating needs, costs and reliability), numerous design alternatives are proposed in early design phase. The analysis carried out in early design phase is to evaluate each alternative given the specification of functions (and possibly architectures), and decide whether they can be taken forward to the next phase (i.e. detailed design phase) that determines on components and technology for realizing functions.

Specific considerations that apply to the early design phase, also considering the impact of complexity and novelty are:

- **Consideration 1:** Only the high-level specification that covers functions that are of highest interest to secure the performance of system is available in the early phase. When a system is too large to comprehend, it is decomposed into manageable parts. Many RAM models are built using this approach, but it seems reasonable to question if this approach is suitable for complex systems with interdependencies. For instance, the traditional model like fault tree represents a system by constructing Boolean logics to represent the failure mechanism of each element [60]. Such representation intentionally neglects the fact that element/functions can interact with each other, resulting in dependencies associated with sequence and structure. Developing the proper models to capture relevant complexity characteristics is therefore very decisive in the early design phase.

- **Consideration 2:** Qualitative models dominate in early design phase, which are unable to reveal the relative difference between design alternative with a sufficient level of confidence [61]. Enabling early trade-off requires more accurate indicators from quantitative models. This requires a pre-processing effort to acquire a holistic understanding of system logic and dynamics, as well as a significant post-processing effort to interpret the calculated results. It is necessary to search for a suitable balance between expressiveness and simplicity of quantitative model in early design phase.

- **Consideration 3:** Novel design concepts add additional uncertainty to consideration 1 and 2. At the same time, the models developed in the early phase are desired to be maintained, updated and reusable when new evidence is collected as design proceeds.

4.2 RAM analysis for early design phase

The right column in Figure 4-2 suggests that RAM analysis is applied in all the phases of system development and its focus and scope vary with phases. Figure 4-3 illustrates the level of activity in different phases of system development. The *planning* phase, which is not illustrated in Figure 4-2, is to set up the project team and collects stakeholders' needs. The RAM analysis tasks for *early design* phase are twofold: (1) formulating RAM requirements on basis of high-level needs (2) verifying whether the formulated requirement can reasonably met by

preliminary[4] design alternatives. The result of early design phase is used to direct engineering efforts in *detailed design* phase to decide the elements that realizes the selected design alternative. The laboratory-based tests and experiments are mainly carried out in the *design validation & verification* phase. The tasks can facilitate the quality control, acceptance tests, reliability growth, system logistics and the like. They may require specific preparations in early design phase but have few relevance to this research project, thus they are not discussed.

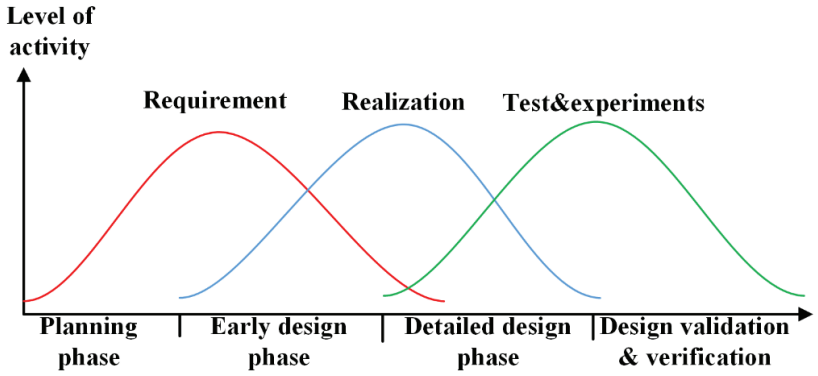


Figure 4-3 RAM tasks along with system development, modified from [19]

In this context, RAM analysis in early design phase can be divided into six main steps as shown in Figure 4-4. It is practical impossible to develop one RAM analysis for an industry-scale system, for instance a nuclear plant or a whole subsea facility. Instead, RAM analysis is built around at different granularity of system. It can continue as far as the lowest level of granularity feasible and then aggregate the results following stated rules.

1. **System familiarization.** It is to define the system concept being analyzed, in terms of operation modes, environment, interfaces and functions.
2. **RAM specification and allocation**. It is to identify RAM requirements. This includes (1) formulating RAM requirement at high level granularity (e.g. system level) given requirement sets formulated by designers, (2) allocating high-level RAM requirement to low level of granularity (e.g. modules/subsystems and components) given defined constraints.
3. **Dysfunctional analysis**. It is responsible to reveal how a system may fail, which that may violate the defined RAM requirements. This includes (1)

[4] The word 'preliminary' is used to indicate the design alternative is only specified at high-level, where only required functions, system structure and IMR for system level are mainly considered.

revealing the cause-effect relationships between failure and specific conditions (2) determining how they may result in a system failure, which is governed by the propagation in a system logic (functional or architecture) frame. The commonly-used models are failure mode, effects and criticality analysis (FMECA), hazard and operability study (HAZOP), fault tree analysis (FTA) and structured what-if checklist (SWIFT).

4. **Failure rate predication**. It is to estimate the frequency of critical dysfunctional behavior. The accuracy highly depends on collection methods and the novelty of system under study. The commonly-used models are part-count technique (estimation at reference point) and part-stress technique (estimation at operating conditions) [62].
5. **RAM modelling and calculation**. It is to calculate quantitative indicators for RAM performance, following the selected mathematical modelling framework. The commonly used models are FTA, reliability block diagram (RBD), Markovian model and stochastic Petri-nets (SPN). RAM modelling is complicated by the complexity of system under study.
6. **Design review and recommendations**. It is to communicate to system designer about necessary improvements and modifications on design and manufacture (e.g. redundancy, stress reduction and changes in IMR strategies).

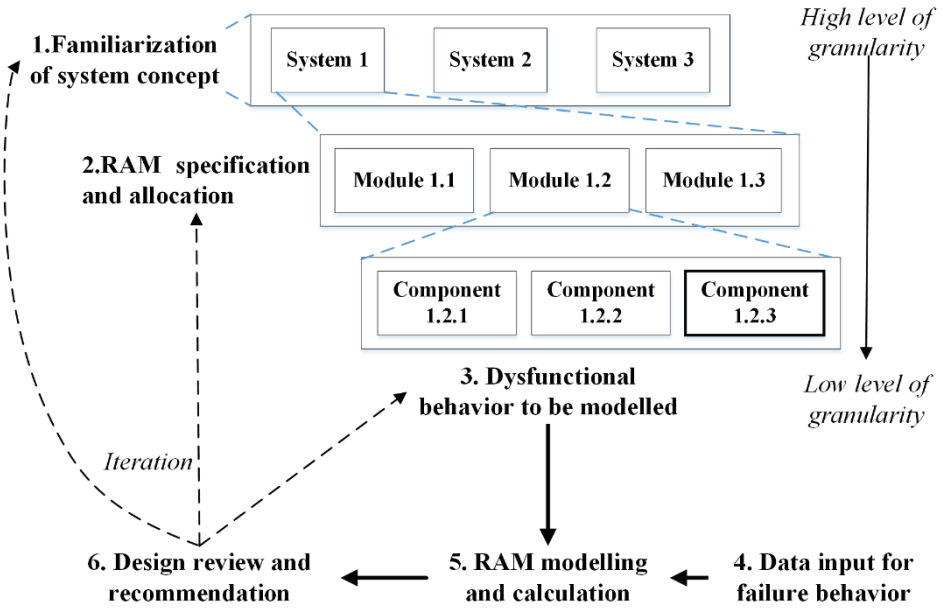


Figure 4-4 Main steps for RAM analysis

All these steps can be model-driven. Using models improves consistency during communication by removing ambiguity in natural languages, and maintains the traceability of analysis [63]. Models are designed to reflect certain aspects of a system at hand, and can be classified based on purposes: (1) the *communication* model with graphical notations and standardized rules to depict the *deterministic* understanding of a system; (2) the *formal* (or computational preferred by some RAM engineers) model follows selected mathematical frameworks for *calculation* and *simulation*. Both of them are available in RAM analysis to drive the work to completion. The selection of RAM models can be a highly individualized process, depends on system complexity, required mastery, commonality and acceptance, and availability of supporting tools [13].

It has to note that one model technique may have different versions and extensions, according the needs of analysis on the certain phase. For instance, FMECA can be performed at functional or physical level. A functional FMECA is preferred in the early design phase as it is easy to implement and only relies on functional specification, whereas a physical/interface FMECA is more frequently used in the detailed design phase and provides more accurate estimation about failure rate [64]. These two versions of FMECA are complementary. Another example could be CCF analysis. In aviation industry, CCF analysis is divided into three parts as practical risk analysis, common mode analysis and zonal analysis, and they are implemented different phases of system development [19]. In the rest of thesis, unless specifying in particular, the model technique is cited in its default version documented in handbooks, standards and guidelines.

This section has accomplished an overview on RAM analysis in the early phase of a new subsea design. Unfortunately, the premise tasks for RAM modelling and itself are completed based on simplifications and assumptions made for given system concept. In this regard, the validity of final results is undermined and the risk of improper decisions is increased. This calls for a proper awareness and consideration about uncertainty, which is the task of next section.

4.3 Considerations about uncertainty

Uncertainty represents the deviations from reality. It seems like a fundamental element remains for RAM analysis no matter how much efforts have been made for understanding system complexity and improving competence in analytical techniques [60]. Uncertainty treatment is therefore essentially a *part of* RAM analysis, to indicate how to judge or present the judgement about the final results in the decision context. This topic is of particular importance in the early design

phase where the level of uncertainty is high while the awareness to the effects of assumptions may be low or not fully investigated.

The rest of this section firstly presents in brief about what forms uncertainty in RAM analysis, where the main contributions are due to incompleteness of analysis, poor data and unsuitable modelling formalisms. Then, it proceeds to discuss the necessary efforts paid in order to minimize the effect of uncertainty in decision-making process.

4.2.1 Classifications of uncertainty

Parry [65] argued to distinguish between aleatory and epistemic uncertainty, according to the source of uncertainty. *Aleatory uncertainty*, also known as 'stochastic uncertainty', arises from inherent randomness properties of the system thus it is irreducible [66]. *Epistemic uncertainty* stems from the lack of knowledge about system being studied, thus it can be reduced as more knowledge is gathered. The combination of epistemological and ontological complexity is the source of uncertainty in RAM analysis.

Related to RAM analysis (or risk analysis in a broader sense), Epistemic uncertainty can be categorized as following according to its types [67-70]:

- **Completeness uncertainty** is represented by what has been omitted from the RAM analysis, including uncovered attributes and uncovered interactions with the environment. Such omission can be deliberate, primarily under the expectation that they are not important, thus denoted as known completeness uncertainty. Completeness uncertainty may be unknown, relating to factors not included because they are (as indicated) not known. The cause of completeness uncertainty can be various: lacking of resources, low competence of analysts and state of knowledge. Systematically evaluating new information during the technology qualification process, for example by adjusting the model and the model parameters, is a way to reduce the effects of completeness uncertainty.

- **Model uncertainty** arises from low suitability of chosen model. Any model serves approximation since it is impossible to include all natural variability of real system [71]. The choice of model depends on the competence of analysts, the recommendation of regulation or standards and specific properties of systems. The chosen model may omit some aspects with less relevance or few aspects with important aspects, given the balance between expressiveness and simplicity. In this sense, model uncertainty is interchangeable concept with known completeness

uncertainty [67]. It can be reduced by increasing validity of model assumptions.

- **Data uncertainty** (or parameter uncertainty) arises from the imprecise numerical inputs for RAM analysis, where the data input could be failure rate, repair rate, perfectness of test, test coverage and the like. The cause of data uncertainty can be the improper methods used for data collection, data estimation and data selection. It can be reduced by using probabilistic tools to quantify the degree of imprecision.

It is worthy to notice that the simplification and assumption made on each step of RAM analysis can significantly contribute to uncertainty. Dysfunctional analysis may give rise to completeness uncertainty, if it fails to identify the full spectrum of dysfunctional behavior. Data acquisition may contribute to data uncertainty if there lacks suitable database or assumptions for using generic database are not reasonably argued. The calculation and simulation may give rise to model uncertainty if the selected modelling formalism cannot properly model the interaction and interdependencies of system elements. The RAM analysts should be responsible to assess these uncertainty and communicate to decision maker, and such process is called uncertainty treatment.

4.2.2 Ways of treating uncertainty in RAM analysis

Uncertainty treatment is not a new topic in RAM community. The main attention seems to have been directed to data uncertainty, as the decision makers usually be aware of the uncertainty arises from bad data and can assess the associated impact within suitable analysis such as uncertainty propagation. The related contributions are Monte Carlo (MC) simulation based methods to generate subjective probability [69, 72, 73] and fuzzy number methods number for representing uncertainty of non-statistical factors [74]. In addition, handling data uncertainty sometimes requires some efforts from high-level perspectives. For instance, the database may be outdated due to the revolution on technology or changes of operating conditions. The improvement on data collection is therefore a cross-enterprise attempt, and requires unified efforts from entire O&G industry including manufacturing and operating companies. It would take decades of effort (considering the expected service time) to truly make a difference in the database.

Some attention has been paid to model uncertainty. RAM analysis needs to make enough valid assumptions to describe the system structure closed to the reality. In this regard, managing model uncertainty (or known completeness uncertainty) is a natural step in the procedure of RAM analysis, but lacking a

structured approach in practice. Zio and Aven [68] have made a clear distinction of different sources in model output uncertainty, and discussed how the model output uncertainty can be treated in risk assessment within various purpose. Continued by this work, Bjerga et al. [75] have proposed a framework to evaluate model uncertainty for probabilistic models. A general method has also been proposed to evaluate model uncertainty by the ability of Bayesian method to update the state of knowledge on the model [76]. Most of the aforementioned proposals are based on numerical methods, few attention has been paid to study the selection of modelling formalisms according to the nature of system behavior.

Despite the importance to give the proper framing and scoping of the analysis, the least attention seems to have been given to completeness uncertainty, some recent contributions are e.g. [67, 77]. Completeness uncertainty is a very useful concept to link to early design phase, where the effect is nearly invisible to analysts and therefore impossible to make the judgement about. Systematically evaluating the system concept at hand, for example by enlarging the scope of analysis or by adjusting the model and the model parameters, is a way to reduce the effects of completeness uncertainty. This is perhaps a better approach than using conservative estimates and judgements, as this approach may be a false comfort if not the causes of why the analysis is not complete are investigated. Here considers models for dysfunctional analysis as example. Not a single model can simply claim a complete set of dysfunctional behavior. To increase completeness of results, some may tend to combine the results from models within different principles, e.g. FMECA that is component-driven and HAZOP that is function-driven. If the underlying principles between implemented models are not recognized by analysts, it may still give to completeness uncertainty thus unplanned rework may be needed. Therefore, by blending the results together may *not* be, in our opinion, the best way to solve completeness uncertainty.

Although completeness uncertainty and model uncertainty hold importance in early design phase, it seems more difficult to address they in the same way as data uncertainty, and screening and conservative analyses are often suggested for compensation [78]. As will be elaborated in this thesis: uncertainty is a concept that goes *beyond* the treatment of probabilities, especially on early stage. Treating (model and completeness) uncertainty is the hypothesis to revisit when proposing new models for RAM analysis in early design.

The next section summarizes the main gaps for RAM analysis, in light of the consideration of uncertainty presented here and major constraints of early design phase discussed earlier.

4.4 Summary of gaps

RAM analysis is continuously confronted by some challenges: the lack of suitable methods to represent and model system complexity, sparse data and information, uncertainty treatment and the like. One recent review work has been done by Zio [60], where the future topics in this research area ranges from old problems for example representation and modelling of multi-state systems, to new challenges with respect to complex systems, e.g. human reliability analysis and modelling of network system.

It is practically impossible to investigate all these topics in one single research work, the interest of this research project is instead narrowed down to the early design phase of a new subsea design. The following points present the gaps with respect to each step of RAM analysis, in the order of importance.

- **System familiarization/design review and recommendation**

Given the *consideration 1* of early design phase, alone many RAM models may not be optimal for representation and modelling of complex system. As discussed earlier, this may result in a twofold design risk: (1) system concept is not comprehended by RAM analysts; (2) the effect of RAM considerations are not observed by designers.

This implies a need for a suite of models to systematically establish an early and continued vision of behaviors, interfaces, elements and control structure for a new subsea system before any RAM specialty model, and the design review is also benefited from doing so. In this respect, this research work takes advantage of another discipline to serve complex systems, i.e. Systems Engineering (SE). Just like RAM analysis, SE is also model-driven analysis to support system design. The SE models use abstractions from three fundamental perspectives (i.e. operational, functional and physical) to manage and maintain a unified version of system complexity along the system development process. Ideally, SE models are designed and maintained by system designers.

While SE models dealing with ontological complexity, a sufficient level of information interface between SE domain and RAM model is needed to deal with the possible epistemological complexity. In order to make it technically possible, it is necessary to advocate a framework that manages rationale and premise of these two domains. SE models are served to support effective and close communication between system designers and RAM analysts and provide continuous feedbacks from/to design team when the early design concepts are being maturing. Yet, the discussion on this topic is sparse from literature and it is

not fully clear about the potential of integrating SE with RAM models to manage the epistemological complexity. Chapter 5 continues on this topic and proposes the framework.

- **Dysfunctional analysis**

One concern for dysfunctional analysis relates to *consideration 1* of early design. The underlying assumption sets of traditional models are challenged when addressed with respect to complex interactions. The traditional models for dysfunctional analysis follow *reductionism*, which fosters *bottom up* approach [45], typically FMECA. In such approach, a system is decomposed to a suitable level of granularity and the behavior at system level is identified by aggregating the behavior of low-level entities. The assumption behind is that low-level entities operated independently and are not subject to feedback loop and interactions are examined pair-wise [45, 79]. Such bottom-up method relies on checklists or guidewords to rigorously identify deviations on *single* entity. The bottom-up model is not efficient for representing a complex system concept, as it may fail to cope with the 'hidden' interactions between single deviations (e.g. failures, errors, mishaps). This inadequacy should be accommodated by *top-down* model that provides a holistic understanding of a system. In addition, top-down model is preferred also in early design phase where the low-level entities have not been embodied or determined.

Another concern relates to the spectrum of contributors is increased in subsea systems built today, as it is being more complex and in particular software-intensive. The increased number of control parameters and unfamiliar feedback loops (see explanations in 3.2.2), not only implies more needs of sensor installation and monitoring, but also the possible failures caused by software errors, improper understanding of specialized operators and flawed functional requirements. It is therefore to develop proper model to recognize and evaluate these potential contributors, otherwise it may give rise to completeness uncertainty of RAM analysis.

Given the two impacts identified above, the commonly used models for dysfunctional analysis may not be suitable to reveal unexpected deviations caused by software controls in the early design phase of new subsea design. The similar problem has already been recognized in other industry sectors like nuclear and aerospace. In nuclear plant or spacecraft, the use of computer-based control is much denser than that of O&G system since the number of components being control (e.g. branching paths of units) is much larger.

Some promising solutions have been proposed by different researchers. One of the most mature models is Systems-Theoretic Process Analysis (STPA) [80]. It

is theoretically feasible to reveal any potential deviations of system behavior, as it is based on *constructionist* point of view that fosters a top-down process. Yet, its use has not been fully exploited in RAM analysis, not because its novelty, nor because it is primarily used for safety analysis, but because it has no interface with RAM modelling and calculation. Therefore, it is not fully clear how to interpret STPA results in communication stage, which leaves designers with challenging tasks to interpret whether the full space of failures is incorporated and to what extent the confidence of quantification could be (i.e. *consideration 2*). Chapter 6 continues to discuss the potential to quantify STPA results and propose our solution by integrating STPA with available modelling formalism SPN.

- **Failure rate predication**

The scarce of failure rate for relatively new subsea system becomes a main limitation for RAM modelling in the early design phase. In reality, there is few reliability database for subsea systems, because the number of subsea systems delivered (even worldwide) is relatively low and each subsea field may require very field-specific adaptions. The data from existing database for proven technology such as OREDA [81] cannot be directly used as input for new subsea design, as there are some variances in maintenance strategies and environmental stresses.

It is therefore required to estimate failure rates based on indirect and inferential information (see explanations in 3.2.2) that can be measured or monitored in all phases of system development. These information that reflect properties related to failure rate, are called RIF (see definition and associated discussions in 3.1.2), such as material of equipment, working load and stress and environmental conditions.

Some practical models have been proposed to estimate failure rate on basis of identified RIFs [82], or update failure rate from generic database by studying the relevance between existing systems and new systems [83]. Yet, they are not able to incorporate one or more following considerations associated with early phase of new subsea design. For a system where complex interactions exist, the mutual correlation between different RIFs can be strong, since they can share some influencing factors, e.g. common-mode connections. The disadvantage of traditional models is therefore the wrong assumption about independencies between random variables (i.e. consideration 1). In addition, RIFs on failure rate may change since new evidence may be collected along with the system development process, for which the selected model must be maintainable in long

term perspective (i.e. consideration 3). The model must be able to update the failure rate estimation when more information is available as design proceeds.

It seems reasonable to suggest developing new methods to overcome the identified weakness. Bayesian Network is the one that gets a lot of attention lately. It can build up the cause-and-effect relationships between the contributing factors, and more importantly it can update the posterior information (i.e. failure rate) when new evidence is available (i.e. new information for influencing factors). Chapter 7 proposes to integrate BN into existing models to incorporate subsea specific influencing factors.

- **RAM modelling and calculation**

There are many different formalisms to complete RAM modelling. Regardless of choice of formalism, the starting is to carry out a dysfunctional model like FMECA then acquire probabilistic information for critical failures. Pressured by the high-level specification of system in early design phase, it seems more feasible to develop Boolean models, such as FTA and RBD. Boolean models employ a hierarchical view thus they are more easily to comprehend by engineers.

The main constraint of Boolean model is the strict assumptions on independence between events. In such setting, test and maintenance events that may have strong impact of probability of failure are not explicitly modelled by Booleans formalisms. For the case where the dependencies are not negligible, advanced modelling formalisms may be selected, such as state transition formalisms. State transition models can account for dependences between events, but they are not easily readable and understandable and their computation time may dramatically increase. Searching for a suitable balance between expressiveness and simplicity is an important topic to investigate in the early design phase. In other words, it is the trade-off between *consideration 1* and *consideration 2*.

ISO/TR12489 [84] has given a guideline on selecting modelling formalism. Yet, it is mainly applied for safety systems instead of subsea production and processing system that operates in various modes. Chapter 8 discusses the applicability of existing modelling formalisms in the early phase of new subsea design, and proposes the updated selecting scheme.

- **RAM specification and allocation**

This topic to some extent relates to *consideration 1*. The model for RAM allocation is to apportion the specified RAM performance to lower level of system, following defined rules. For instance, the component with highest failure

(alternatively lowest reliability) is assumed to have greatest potential for improvement. Yet, traditional models for RAM allocation are for generic use, without considering the complexity of subsea systems. For a complex subsea system, the defined rule may be invalid or have less practical meaning. For instance, the components with different failure rates may locate on same module so they are subject to the same IMR schedule, it is therefore no longer feasible to consider the reliability improvement on single component and effect of failure must be embraced as whole. Moreover, few allocation models seem to capture non-functional issues, such as weight, physical design constraints. The possible extension of allocation methods to add new factors of relevance to subsea may be of interest. Chapter 9 presents a review of available RAM allocation models and suggest for selection criteria under subsea complexity and possible extensions needed subsea.

PART II: MAIN RESULTS

Chapter 5 Proposed framework for RAM analysis

Understanding and studying how a complex system works (or fails) requires a holistic view about the system, its parts, and their interactions. SE is the discipline that develops models to understanding a system from different perspectives, and the ability to do so requires integrating background knowledge and information from multiple disciplines including RAM.

This chapter presents our contribution on merging SE with RAM analysis, which is given as a new framework that details *how* RAM analysis is incorporated in a design process with the support of SE models. It begins with introducing SE, including the body of knowledge, used models and the often cited topics related to SE. On basis of this, an outlook on integrating SE models to RAM analysis is presented, plus some discussions on similarities and difference of SE domain and RAM domain. Then, the main result for this topic, RAM-SE framework is presented to show how RAM analysis as a specialty engineering activities can be benefited from SE. In the end, a real world subsea design case is presented to demonstrate the application of RAM-SE framework.

The main content of this chapter is based on the published article [85] as well as conference paper presented in RQD 2017 [57]. They are prepared as part of this PhD project, see the appendices for original content.

5.1 Theoretical foundations

This section starts with origins and evolution of SE, which are of relevance for SE definition and professional development. The core of SE is explained to evaluate the potential for using SE as the foundation for framing RAM analysis.

5.1.1 Systems engineering

SE is *'an interdisciplinary approach and means to enable the realization of successful systems.'* [86]. The term *realization* implies that this discipline focuses on the entire life-cycle for system of interest, and the term *system* refers to the large-scale and complex socio-technical system. SE was originally adopted in Bell Laboratories and US military standards, and has been increasingly practiced in many other industry sectors since World War II. As a result of joint efforts from practitioners and researchers in the profession of SE, International Council on Systems Engineering (INCOSE) has been established in 1995. The SE handbook published by INCOSE [86] contributes to address SE concepts, models and practices that manage complexity arisen from diverse engineering and engineering management disciplines.

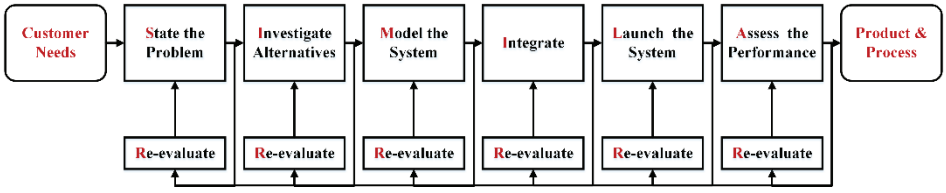


Figure 5-1 SIMILAR process, adopted from [87]

Literature is abundant with definitions of SE, see, e.g. [88-90]. Among them, there are two essential concepts embraced in SE: *systematic* and *systemic* [91]. *Systematic* refers to the way of solving complex problem, i.e. iterative and stepwise *process* for problem solving. A SE process includes the integration of all anticipated disciplines in the life cycle of an operational system, to understand and determine the system performance considering operational, functional, physical and other constraints [89]. A myriad of SE processes have been proposed, for example SE process adopted in standards IEEE-STD-1220 [92] and MIL-STD-499 [93], SIMILAR [87] as shown in Figure 5-1 and SPADE model [94]. Despite the difference in tool-kits, criteria and scope of focus, all SE processes include generic steps to analyze the real needs of problem, describe the system and requirement, model and analysis the system, specify the solution and test and evaluation. *Systemic* refers to the way that the thing being studied, means that the problem or a set of problems are viewed in its entirety [90]. As opposite, a non-systemic analysis divides the whole problem into individual parts that are 'easy to solve or analyze', where the interactions between each part are hardly taken into account or some interactions are easily ignored. A systemic approach expands the scope of problem being studied and increases the potential to provide a feasible solution. For instance, the traditional RAM analysis focuses on the physical (hardware wise) system. However, with the evolution of technical system built today, software, human and other organizational factors are considered as the essential part of a system, and their interactions are becoming the resource of failures. These two features make SE feasible in managing and organizing complexity, both from ontology and epistemology perspective.

Two professional development related to SE are introduced in the following, given their relevance for discussion later.

- **Model Based Systems Engineering**

Model-Based Systems Engineering (MBSE), as the name suggested, is a process that extensively uses models to capture more substantive defects and create more feasible solution in SE activities, e.g. developing the consolidated system concept [95]. One important feature for MBSE is its layered process,

where model is developed with increasing details and converge strategically to produce solution, along with the system development process.

In MBSE, the system concept can be viewed from more than one perspective. Figure 5-2 illustrates MBSE process that captures the operational, functional (or behavioral), physical (or architecture) aspects of the system being evaluated, with the support of a rich set of model notations. As shown in Figure 5-2, the emphasis of each domain is traceable through the models using consistent language. If any changes are made on any domain, the impact on the adjacent domain can be easily revealed.

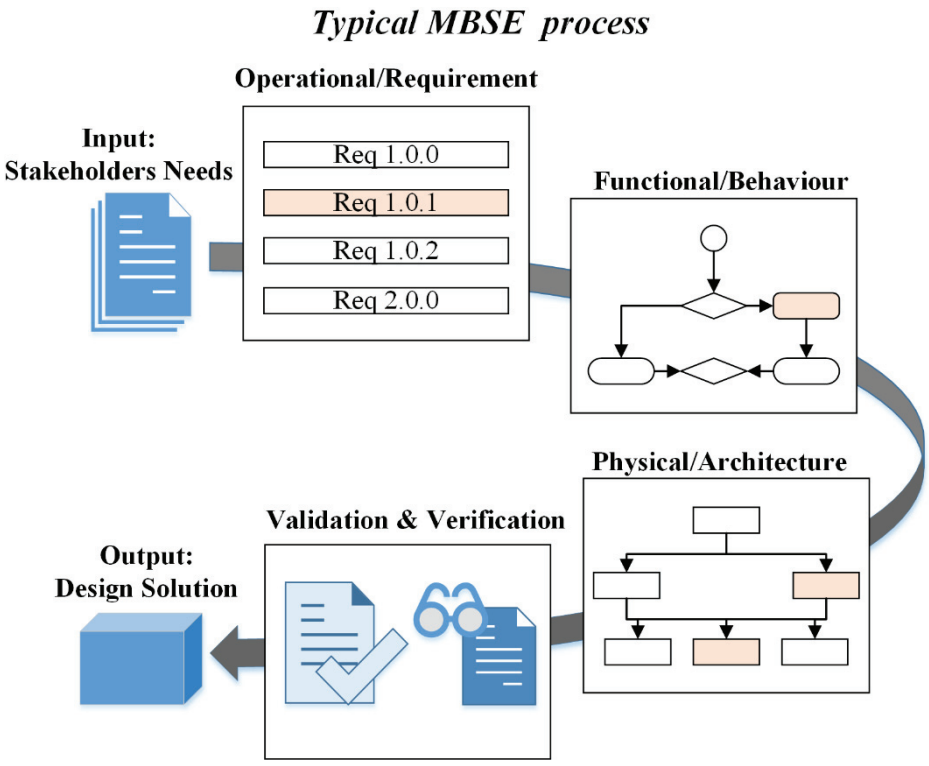


Figure 5-2 A typical MBSE process

There are numerous models to represent the view of each domain. Here considers functional/behavior domain as example. The commonly used graphical models are Function Flow Block Diagram (FFBD), activity diagram, N2 diagram and sequence diagram. They are much different in representing the behavior or function. For instance, FFBD focuses on representing the control structure but no data flow, whilst sequence diagram focuses on data structure but no control. The traits of these models are briefly described and discussed in literature [95-97]. For

a rather linear system, sequence diagrams are preferred to clearly communicate to stakeholders that how a production process can be completed step-wise. For a system that involves various controls parameters especially when control is decentralized, FFBD may be more feasible to give an impression about how each entity interacts with others.

System Modelling Language (SysML) [98] is a commonly accepted toolkit for MBSE, which uses the same profile mechanism as Unified Modelling Language (UML) with some extensions made to give support to SE activities. Currently, there are nine types of graphical models for SysML, including activity and sequence diagram mentioned above. Most of them can provide more than one perspective to depict system behavior, system components and system requirement, and the difference is reflected by the level of details, content and the use.

- **Systems Thinking**

Systems thinking emerged as a response to the rapid increase in complexity of technical systems. In principle, it denotes the way of thinking following systems theory: system is more than sum of parts. System thinking allows having a holistic and complete view on solving the problem: identify the individual behavior and study the systemic correlations within [99].

Systems thinking could be the underlying foundation for many analysis and models, with respect to the needs of analyzing and handling complexity, given two assumptions [79]. The first assumption is that the engineering effort for improvements on an individual component may not lead to an overall optimization. Returning to RAM analysis of new subsea design case, some subsea equipment cannot be replaced without pulling a whole module. This means that the effect of failure is not isolated to one component and one system function alone, but may include many others as well. Therefore, the individual improvement on RAM of component may not improve the overall RAM performance. The second assumption is that the performance of individual component cannot be understood without considering internal and external interactions. For instance, subsea operation involves a high degree of automation and process control as manned actions have been dramatically reduced or eliminated in the subsea environment. This implies some errors are related to inadequate operation, flawed control process and missing or wrong interactions. In this circumstance, analyzing failure caused by physical degradation is no longer considered as sufficient practice of RAM analysis for new subsea design.

In summary, SE is used to integrate all disciplines into a team effort, thus it can be adopted by system designers in subsea design environment. One question is

therefore raised: *is there any potential for using SE as the foundation for new RAM practices, based on used models and concepts?* These two expertise domains share some similarities and difference. They both employ models developed to give an abstract view about same system concept, albeit for different analysis needs and have different roles in the development of a system. As discussed earlier, Carrying out SE analysis before RAM analysis may improve the consistency of understanding and facilitate the construction of RAM models. The next section is based on this vision, to present a comparative study about used concepts and produced models of these two expertise domains.

5.1.2 Integration of SE and RAM

According to SE handbook [86], RAM analysis can be regarded as a specialty subset of SE, even then, it seems that the specific interfaces between SE analysis and RAM analysis are given limited attention. A review of the literature uncovered references that discuss the potential integration and proposes some tools to support exchanges between RAM and SE. Jigar et al. [100] presented ways to extend the existing availability allocation process to the relevant stakeholders involved by applying a SE approach. The work indicates that the availability allocation problem can be re-designed within SE principle so that the analysis is conducted in an iterative and systematic manner. Garro and Tundis [101] showed the possible extension of reliability analysis of a system to that of the System of Systems (SoS) concept, to solve the main issues arising in system reliability analysis considering particular properties of SoS. Shainee et al. [102], apply SE to the design of a technical marine SoS, while Ramírez et al. [103] discuss ways that SE serves in coordination and communication by alleviating potential friction between multidisciplinary actors.

As concluded in Chapter 4, the current RAM practice may not be optimal for complex system design characterized by highly coupled parts and non-linear interactions. Table 5-1 gives detailed examples when facing complex and indicates the suggested requirements to a new RAM analysis.

A relevant candidate to support the realization of these requirements has been identified within a new framework that includes SE to improve the basis on which the RAM analysis is carried out thus support design team coordination. Therefore, the pursuit of integrating RAM concepts along with the design process is realized by transferring between SE artifacts to analytical methods that solve the RAM-related problem. A SE artifact is a set of models that capture different levels of abstractions (i.e. operational, functional and architectural) of design, where RAM models inherit the same view with adjustments made due to accommodate the selected mathematical framework.

Table 5-1 Foundations for new practice of RAM analysis

Identified weakness of existing practice	Desired features
Many RAM models are not alone well suited for identifying and studying the effects of complex interactions. Such practice results in some design risks that stem from insufficient considerations of engineering aspects, and will be latent on the day one of operation. **Example:** Functional/physical breakdown are often used as reference to performance functional/physical FMECA. The failure is only identified and evaluated on the selected hierarchical decomposition. Such 'system concept' developed by RAM analysts does not explicitly express any dependencies.	Need to master complexity of design concept in a systematic and organized way before constructing any specialty RAM models
Probabilistic models dominate in most practice, which leads to fact that the results of RAM analysis could be misinterpreted or misunderstood [104]. **Example:** In the case of a new subsea design where software and communication technologies are used to implement a majority of the functionality, many failures are systematic (see 6.1.1 for detailed explanation) rather than the result of individual parts' degradation. Such failures may not be sufficiently covered in RAM modelling.	Need to communicate the result of RAM analysis in other ways than probabilistic based indicators so that systematic failures can be correctly communicated.
(Model-based) RAM analysis are often 'disconnected' from design process or have little interface with other engineering disciplines. It is therefore not ideal for engineers with different backgrounds to capture the useful concepts in their own models and analysis. **Example:** In some practices, some may argue that RAM performance is the 'obvious' result as long as system designers do their jobs properly.	Need to integrate RAM analysis with the artifacts produced by other design contributing teams by connecting the produced models and used concepts.

Figure 5-3 presents a conceptual map that highlights three core elements for the framework: SE models, RAM models and design concept itself. SE models constitute the basis of system design, whereas RAM models provides effective means to identify how a system that expected to run properly can fail. In this respect, SE models should be a prerequisite for developing RAM models, and the consequent implications of RAM models influence the development of design concept by incorporating RAM aspects that extend most of design models based

on SE tools. The next section elaborates on SE activities with an outlook on RAM integration.

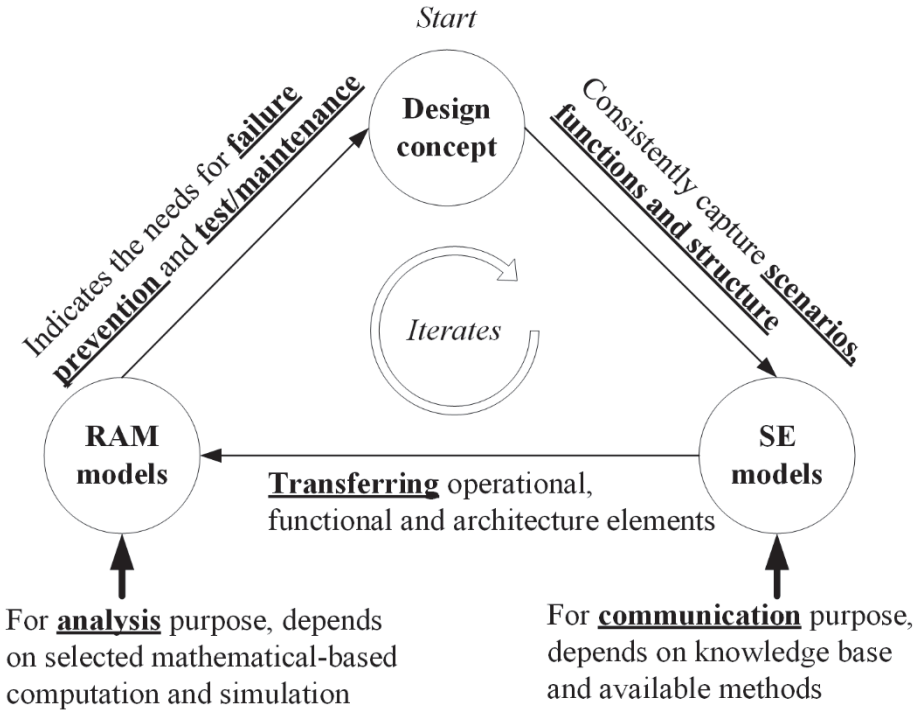


Figure 5-3 A conceptual map of RAM and SE models

5.2 Applying SE to integrate RAM in design

SE engineering process mainly proceeds sequentially by analyses with four perspectives, i.e. operational, functional, architecture, and verification and validation [95]. RAM analysis, as the 'simple' verification and validation work, needs to extract the information from the first three analyses.

5.2.1 Operational analysis

The SE engineering process starts with identifying stakeholders needs [86]. As stated before, both RAM analyst and system designers who maintain a unified vision of the system concept are the primary stakeholders in new subsea design. On basis of stakeholders needs, operational analysis aims at a preliminary overview to describe system missions, operating environment and the internal/external interfaces.

The typical models used for operational analysis are *context model*, *sequence diagram* and *use case diagram* [95]. Context model is to define the boundary (or perimeter) of a system and its environment and illustrate how the element of a system interact internally and externally [96]. An example of context model is Figure 3-2, where the *system* refers to the process of a new subsea design instead of an engineering system. Use case diagram is to use scenarios to describe how to a system, which helps in eliciting functional requirements. Use case can be developed in form of text or graphical notations, the latter one is called as use case diagram in SysML. Sequence diagram is to visualize the interactions (e.g. message exchange, processing and command) between different elements of a system associated with time dimension. Compared to use case diagram, sequence diagram is a more explicit description of functionality along with scenarios, for this reason it can be also considered as functional analysis. Given the objective of operational analysis, context model is always required to characterize the interfaces crossing boundary, and system missions can be depicted by either use case diagram or sequence diagram if reasonable argument is made.

The results of operational analysis is used to formulate contractual requirements. For example, with SysML one can model the text-based requirements supported by these diagrams together with a requirement table to clarify their relationships in the design [105]. The formulated requirements consists of two groups: functional requirements that define what system should do, non-functional requirements that details about performance of a system when functional requirement is fulfilled, such as weight, size, safety and RAM. The verification work associated with each set of requirements are carried out separately, namely design analysis and RAM analysis. The introduction or update of RAM requirements needs to update functional requirements and vice versa, but there are many constraints, such as schedule, budget and difference in background, on the simultaneous updates. It implies a need of a communication platform to exchange the information and concept obtained through produced models for eliminating possible inconsistencies in maturing the design itself.

5.2.2 Design analysis

Design analysis is to generate the design alternatives with respect to functional requirements obtained by operational analysis, and study them by analyzing their functional and physical aspects.

- **Functional (behavior) analysis**

The function analysis is a structured process of visualizing how the system achieve its intended gains. In RAM community, the basic model for function analysis is the *functional decomposition* (or called as functional tree analysis),

which is a *static* representation of the hierarchy structure of functions. Such tree-like decomposition is often criticized as it cannot give the systemic view showing how the functions are coupled. The other graphical models like Structure Analysis and Design Technique (SADT) and Quality Function Deployment (QFD) are also commonly used [106].

In SE community, different types of functional models are categorized as *flow-based* and *event-based*, and their representatives in SysML are *activity diagram* and *state diagram,* respectively. As a specialized form of flowchart, the activity diagram uses 'tokens' to illustrate the concurrency of flow of control and data. This semantic aligns the structure of activity diagrams with that of Petri-nets accepted in RAM community, although the activity diagram is more concise than standard Petri-nets, especially when it comes to modelling the reactivity of workflow [107]. Considering the needs of quantitative notations, different mapping methods are proposed to translate UML activity diagrams to Petri-nets [108] or SysML versions [109]. The state diagram (or state machine diagram) explicitly describes the dynamics of an object or system. It consists of potential states and triggering events that drive the transition between states. The state diagram resembles Markov chains, preferred in RAM community on the surface, but with the distinction that Markov chains as the formal model based on strict mathematical framework represent less content state diagrams. For instance, when transferring a state diagram to Markov chains for quantitative modelling, synchronization and parallelization of state diagram are abstracted away. The flow-based functional model and the event-based model are intended to be consistent; i.e. if all transitions on a state diagram can be triggered by the completion of activities, then the context captured in activity diagram and state diagram are consistent. Activity diagrams based on flow of control are better used for modelling a process of operation, whereas the state diagram emphasizes events.

There are other models that are not covered in SysML that also support functional analysis. For example, FFBD is used to represent the control structure and emphasizes the sequence of a successful operation. Figure 5-4 illustrates how a subsea gas compression can be modelled by FFBD. FFBD emphasizes the controls of subsea gas compression process but no triggers, it means that analyst cannot tell the sequence among the function of 'safety control' and the function of 'lubrication' from Figure 5-4. To overcome such limit on representing behavior spectrum, FFBD is often implemented in conjunction with event-based models, in order to encompass the nature of triggering [88, 95]. In similar fashion, these graphical notations ease the communication of conditional system behavior between designers and RAM analysts even when no corresponding methods are found in RAM community.

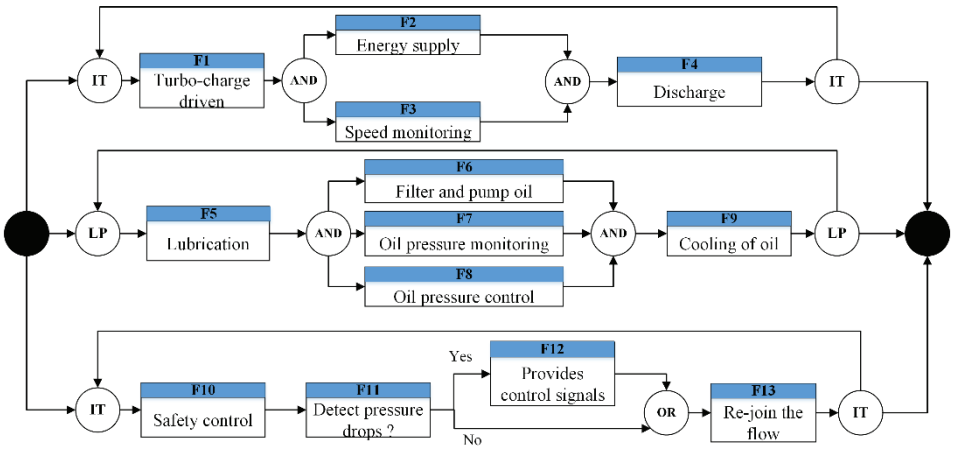


Figure 5-4 FFBD for subsea gas compression

- **Physical (architecture) analysis**

The physical (architecture) analysis defines the components that realize the identified functions. Depending on the role RAM analysts have in the design phase, a technical system is generally considered from a functional instead of architecture point of view. However, it shall not be the case for new subsea design. Even if the well-rounded functional analysis is completed, analysts may not be able to evaluate the potential failure modes due to the incomplete view of given system concept.

The most commonly used approach to study physical aspects of system is the physical decomposition, which is often used as the 'checklist' for the dysfunctional analysis, such as physical FMECA. However, such breakdown structure does not help in the context of complex system as many parts are interrelated and ought not to be analyzed individually. Often times, studying physical aspects in RAM community is a brainstorming process that requires participations from multiple disciplines, e.g. HAZOP.

Using SysML, one can generate block definitions that contain physical attributes such as weight and size and they can also inherit attributes from other (higher-level) blocks. In such practice, building physical models of a subsea system can ensure coverage and traceability of defined constraints and assumptions (e.g. height, width, mass and the like). However, relying on the requirement table provided in SysML only gives an indication about constraints. The lack of 3D model can be compensated by using Computer Aided Design (CAD) tools when needed. The complete architecture analysis can assist in understanding how the local effects on basic components can disturb the system

and updating stochastic descriptions of unwanted events, together with expert judgments and experienced practices, for example, using Finite Element Method (FEM) to study the failure rate of a pipeline considering the effect of sand, fluid composition, ambient temperature and pressure.

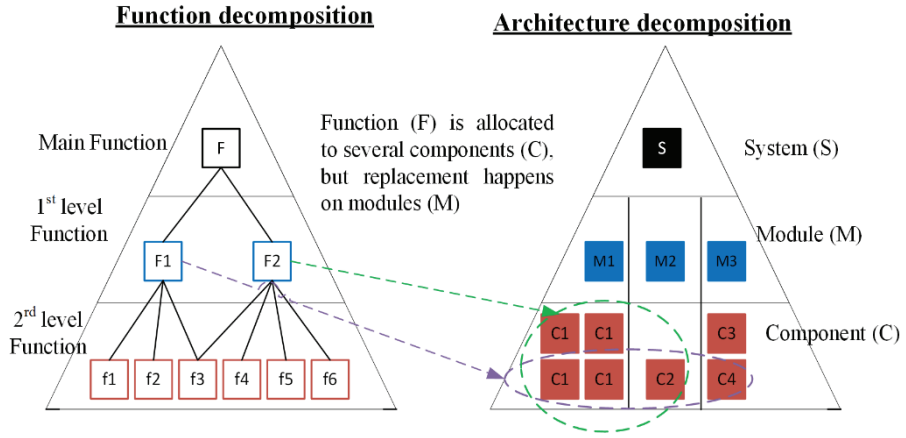


Figure 5-5 Modularity of subsea design

It has to note that details about components and parts are not settled in the early design phase. In this respect, the aforementioned approaches for physical analysis are much more meaningful in detailed design phase than early design phase. Yet, some physical and architecture deserves attention even in the early phase of subsea design, such as modularity of new subsea design. As illustrated in Figure 5-5, some subsea functions are realized by components located within different modules, but the replacement takes place at a module level. Design Structure Matric (DSM) is often used in SE to handle the modularity replacement problem [110]. DSM is efficient in organizing the interactions between components and visualizing the shared patterns, and it can help designers to identify the relatively independent modules. Even though DSM is not available in SysML, it is recommended for new subsea design to support RAM analysis tasks such as RAM allocation.

Another attention may be paid to zonal stress posed by proximity and sequential production steps. The local failure may increase the stress on the other adjacent components due to proximity. This issue has received attention in aviation industry and zonal analysis (ZA) has been proposed to manage it [19]. ZA have not been fully exploited in O&G sector yet, but one can foresee this model that exclusively incorporates physical properties is meaningful as subsea modules are designed compactly. For example, the leakage of a pipeline can cause

gradual contamination in neighboring areas. Such effects must be considered in RAM analysis, for example failure rate estimation.

5.2.3 Trade-off analysis

This analysis is not tied with any SE perspective, but it is recognized as an important step in SE activities. Multiple conflict objectives are typical in an engineering design process. For example, the choice of materials to guard against internal corrosion in a pipeline may improve the reliability but may reduce the efficiency of production (i.e., OPEX). Decisions are needed to find a balanced solution considering all the assumptions and constraints.

Trade-off analysis is ideally suited to design review and recommendation in the early design phase, and iterated for several rounds before finding the best possible solution. As stated clearly in delimitation, the commonly-used techniques such as analytic hierarchy process and other techniques preferred in SE (e.g. [111]) are not discussed in this thesis. However, one should remember that quantification of all the factors identified in the dysfunctional analysis is nearly impossible. Establishing a set of scenarios (e.g. accidental scenarios and maintenance scenarios) is always considered as the supplement to communicate the implications on design. The subjective judgements are largely implemented in such analysis. The discussion is continued in 0that proposes new model for dysfunctional analysis.

5.3 RAM-SE framework

The proposed framework shown in Figure 5-6, has been named RAM-SE to highlight two expertise domains involved in subsea design environment. The RAM-SE framework revisits the current process of RAM analysis, and proposes the steps integrating artifacts from both SE and RAM expertise domains.

- **Step 1: Operational analysis**

The main objective is to systematically formulate RAM and functional requirements based on the needs of identified stakeholders. This frames the scope and paves the ground for both design analysis and RAM analysis by abstractly characterizing the life cycle, interactions and externals of the system in question.

- **Step 2: Design analysis**

Design analysis assists in the systematic establishment of the design concept and supports the effort to understand and organize the system structure. RAM-SE uses often-cited methods from the SE community to establish the system

architecture. The advantage for having design analysis is to efficiently eliminate the inconsistency caused by the variations in competence, knowledge base and experience of RAM analysts. The highlighted methods in Figure 5-6 only consider subsea design environment. The refinement and complement of tools for design analysis should consider following criteria: system complexity and novelty, commonality, availability of software-based tools, plausibility as well as the correspondence to RAM tools.

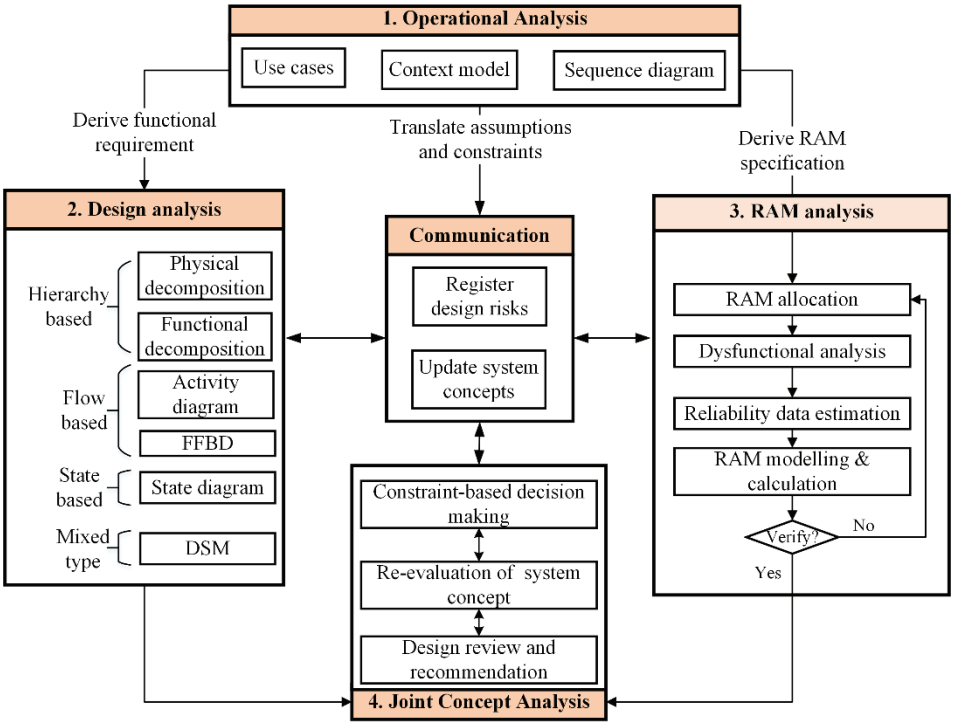


Figure 5-6 RAM-SE framework

- **Step 3: RAM analysis**

RAM analysis in this framework contains only *four* steps identified in Figure 4-4, since the rest of this framework concerns '*familiarization of system concep*t' and '*design review and recommendation*' in favor of SE models. Table 5-2 summarizes RAM models used for these four steps, and specifically discusses the possible extensions and advantages based on SE models. As always, the proposed methods in the framework should be updated or replaced based on the real analysis of needs.

Table 5-2 Advancements for RAM methods in SE context

Methods	Objectives	Extensions based on SE models
FMECA	- Uses a basis for detailed RAM analysis and maintenance optimization and planning - Document the effect of failure on system	- Systematically identify all operational modes and functions attached to each potential failure modes - Carry out an extended/revised type of FMECA that is able to involve dynamic aspects of key scenarios, see also the discussion in [112]
HAZOP	- Review all system sections for abnormal operational situations for all modes of operations - Identify hazards and hazardous situations that must be encountered for or removed from design concept	- Be less resource and time consuming - Instead of brainstorming, focuses on the solid system architecture to evaluate the possible hazardous situations
Maintainability analysis	- Establish maintenance strategies before put into the operation [113]	- Incorporate operational and maintenance mode in the design analysis - Develop the subsea system-specific or module-specific maintenance strategies
CCF assessment	-Encounter common mode errors that lead to the loss of independence	- Systematically indicate the possible dependencies among functions and system architecture, such as proximity, overlaps in functionality, and dependencies on resources (e.g. data, information and power supply)
Zonal analysis (ZA)	- Encounter the malfunction that could result in serious effects on the adjacent components	- Benefit from building a consistence system architecture that incorporates physical properties
RAM allocation	- Decide the necessary improvement on component level to achieve the minimum required RAM performance in an optimal way	- Benefit from building a consistence system architecture that considering modularity or other architecture aspects that may influence the efficiency of component improvement, e.g. DSM

Failure rate predication	-Provide failure rates and other input parameters for reliability modelling and calculation	- Integrate a comprehensive set of influential factors on identified failures brought up by design analysis - Involve subsea designers as the experts via joint concept analysis for judging upon some particular issues, such as the excess of working loads, variations in internal or external pressures
RAM modelling and calculation	-Prepare a set of suitable models to be used for reliability and availability analysis - Identify relevant failure scenarios and evaluate model capacity in light of defined events	-Identify the characteristics of architectures (e.g. modularization, obsolescence and degradation) and scenarios/events (e.g. delay on repair, imperfect testing or harmful testing, failures of activation of backup) needed to be considered in suitable modelling approaches.

- **Step 4: Joint concept analysis**

This step is an important step that helps ensure sufficient interfaces between the design analysis and RAM analysis and appropriate follow-up actions. The objective of joint concept analysis is to present some common themes that cannot be solved or considered by any individual engineering discipline. This therefore requires the involvement of RAM analysts and designers to accumulate results from discipline-specific analysis and decide on necessary follow-up based on the design implications of analyzed results. Some scenarios generated by RAM analysis may imply modifications of the existing design concept. Constraint-based trade-off checks whether the recommendations made based upon the results of RAM analysis are economically, technologically and operationally feasible. For example, lifecycle cost analysis, sensitivity analysis and technology evaluation must be conducted.

- **Communication**

The communication block is centrally located to indicate its importance during all steps of RAM-SE framework. Communication is indispensable to link the separate contributions of the two expertise domains. The multiple players involved in the design process must agree on the 'disagreement', and continuously evaluate the proposals from others. Effective communications should take place to ensure that all stakeholders understand the basis on which decisions are made and the rationale behind. The term *design risk* here refers to

the simplifications and assumptions made by RAM analysts, as well as the lack of information (from system designers) to support relevant RAM analysis[5]. Then system concept configuration baseline should be based on both the contributions from RAM analysis concerning potential occurrence and damages, and tradeoffs related to the system structure formulated in design analysis. Every revision should be registered and updated.

5.4 Case study: subsea fiscal meeting system

This section introduces an existing design concept-fiscal metering system to demonstrate the application of RAM-SE framework. The fiscal metering is one vital part of SGB to precisely measure petroleum product exported from delivery to the eventual recipient. The accuracy and validity of flow measurement are very important for contractual obligation between custody transfer parties (e.g. consumer and supplier).

5.4.1 System description

Equinor [114] has proposed a design concept for subsea fiscal oil export system using ultrasonic flow meter (USM), a schematic is presented in Figure 5-7 that consists of sampling module and metering module. The sampling module includes sampling devices (QS) and pumps. When the oil exported from subsea storage passes the sampling module, a representative amount of oil is extracted by sample probe. The pumps are installed to provide sufficient power for lifting the sample to the dedicated facility located topside via umbilical. The metering module consists of USMs, pressure transmitters (PT) and temperature transmitters (TT). When the oil is routed into pipeline of metering module, the volumetric flow rate, pressure and temperature of flow can be measured. USM, QS, PT and TT can be duplicated for back-up use and improvement of monitoring capacity. In this design concept, one metering run contains a duty USM, a master USM and a spare USM installed in series. The installation of multiple USMs enhances the ability of monitoring the quality of meters and reduces the measurement uncertainty if the resulted measurement is the average of readings from different USMs. The spare USM serves as redundancy to both master USM and duty USM. The metering module is considered as fully functional when two flow meters are available, where the spare meter can serve as duty or master when needed. The control system is located on topside to control the operation of sampling module and metering module. SEU is installed to distribute the necessary coded control command to each instrument and collect the data for further transmission to other subsea units or control system. Assuming that

[5] This topic is revisited when reaching specialty steps of RAM analysis that discussed in later chapters.

duplicated SEUs are installed in the metering section to ensure the long-term stability. All the equipment are connected to two SEUs so that there are redundant communication passes for metering station.

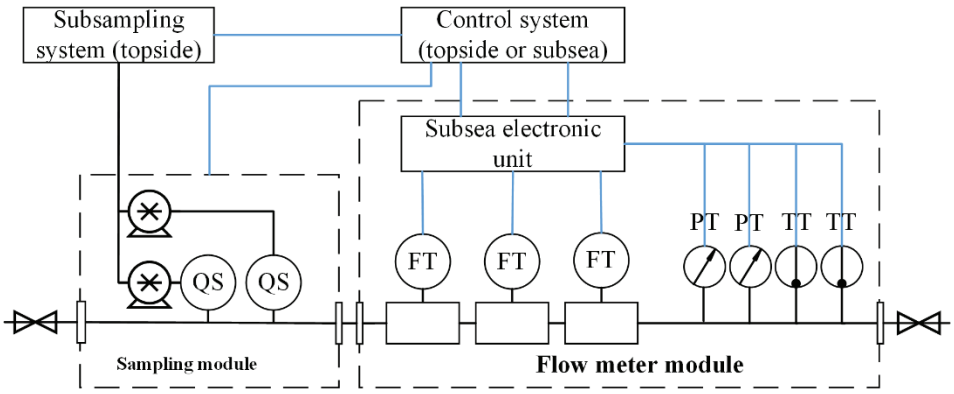


Figure 5-7 Subsea fiscal oil export metering system, adopted from [114]

The validity and accuracy of signals from USM, PT and TT may lessen after installation due to various factors such as outdated calibration, bad piping conditions and physical damage of parts. This design concept is assumed to function in spite of failed PT and TT, since the loss of pressure and temperature measurement can be compensated by other transmitters adjusted by calculations. When there is a need to replace the USM, the metering station should be lifted through the rig and re-calibrated at the accredited calibration laboratory. Replacement of USM causes an interruption of production as the downtime of metering station is significant.

This design concept includes many parts including PT, TT, valve connection and tubing that have been qualified for subsea applications, except the USM. The following presents the evaluation of this design concept following the key activities in RAM-SE framework, where the main focus is directed to RAM performance of this design concept and necessary adaptations considering subsea conditions.

5.4.2 Operational analysis

- **Define the boundary of USM assembly**

Figure 5-8 presents a simplified context model for describing the surrounding elements (i.e. blocks with grey) of USMs (i.e. the block with black) and associated interfaces, in order to share this core concept agreed by various stakeholders.

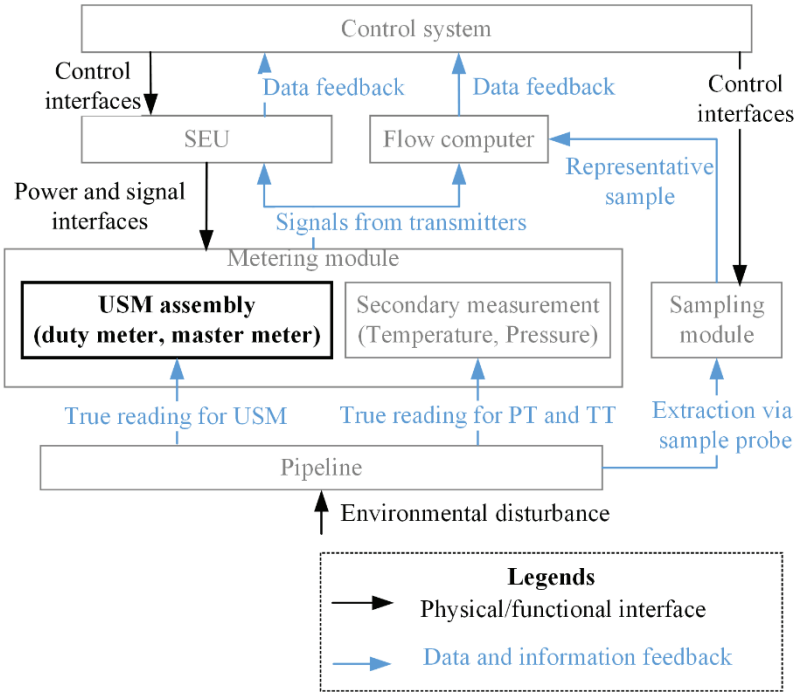


Figure 5-8 Context model for USM design case

- **Identify functional and RAM requirements for USM assembly**

The major need from stakeholders is to ensure the accuracy of USM readings against potential deterioration and expected variations from externals. The functional requirements can be elicited by analyzing the interfaces in Figure 5-8. For instance, factors related to the reading and calculation of USMs are setting of flow computers, readings of PT and TT and on-site master prover. In addition, environmental conditions on metering site (e.g. ambient temperature and pressure, humidity), piping arrangement and thickness, and power and signal interfaces with electronic units, all can impact the performance of USMs. These functional requirements result in upgrading or detailing the existing design concept. For instance, the uninterrupted power unit may be needed by the flow computer to avoid possible power outages that cause the loss of data. The Norwegian measurement regulation requires the uncertainty to be less than 0.3% of standard volume. Given the analysis of current laboratory result, the uncertainty of this design concept is estimated to be less than 0.2% of standard volume at 95% confidence level [114].

Considering the expensive retrieval and intervention, the RAM requirement agreed by stakeholders is: '*not a single failure on USM can require the retrieval*

for calibration and adjustment during 20 years' service time'. Consequently, a degraded performance of the flow metering module may be acceptable, which means operator may not immediately shutdown the flow metering module if two out of three USM outputs are lost. Assuming that uncertainty contributions from each USM are uncorrelated, the resulting measurement uncertainty approximately equals the reciprocal of the square root of the number of meters. For instance, if the measurement uncertainty is estimated as 0.15% for a single USM, the resulting uncertainty for two and three USMs are 0.11% and 0.09% respectively.

5.4.1 Design Analysis

- **Generate various design alternatives for USM assembly**

Based on Figure 5-8, it is assumed that each functional channel that fulfills the operational needs requires the signal interfaces between USM and SEU. There are two alternatives for system configuration: configuration 1 is that all three USMs are connected to two SEUs, and configuration 2 is that one USM is connect to SEU and other two are connected to another SEU. When there is a failure on a SEU connected to two USMs, the whole metering station loses two signal inputs from the USM assembly. Configuration 1 clearly offers higher operational flexibility as the SEU is fully redundant for each USM, at the same time introducing more complexity to the system due to the increasing number of jumpers. The failure of jumpers can cause jammed, interrupted or missing signals, which can immediately cause an increase of measurement uncertainty and the need for maintenance. The maintenance of USM assembly includes several tasks such as full isolation of the metering station from the pipeline, removal of hydrocarbon in the units of metering station and lift of whole metering station through the rig. The length of downtime related to maintenance activities of USM assembly is assumed as 2 months (i.e. 1440 hours). The faulty SEU and jumpers (i.e. flexible connection between units) can be restored in one week (i.e. 168 hours) after two signals from USM are lost.

To compare various maintenance strategies for USM assembly, the three possible maintenance strategies are as follows given the considerations from system designer.

- Strategy I: The activities related to maintenance starts immediately when two USM functions are affected, the metering station is shut down during maintenance.
- Strategy II: The activities related to maintenance postpone one year (i.e. 8760 hours) when two USM functions are affected, the metering station is shut down during maintenance.

- Strategy III: The activities related to maintenance starts immediately when two USM functions are affected. At the end of lifetime (i.e. the last 5 years before intervention), it is acceptable to operate metering station with only one USM.

The three maintenance strategies imply different RAM performances for the given design concept. The insights to maintenance management had not been discussed in the prior versions of the design proposal from [114]. Considering two possible configurations and three different maintenance strategies, there are six cases in total to proceed in subsequent analysis.

- **Analyze functional and physical aspects**

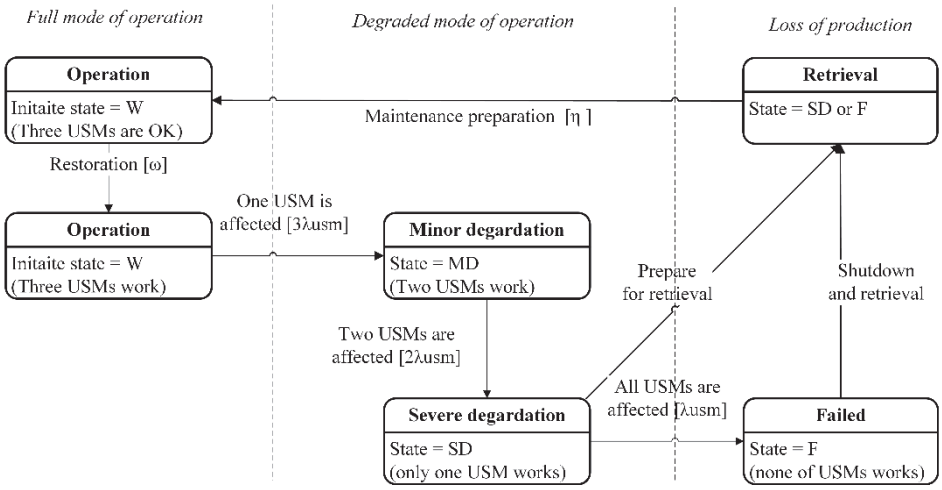


Figure 5-9 State diagram for USM design case

Figure 5-9 presents a state diagram to study functional dependencies realized by transition among different phases (i.e. retrieval, normal operation) in the lifecycle of USM assembly. In Figure 5-9, transitions including '*component failure of USM*', '*prepare for retrieval*', '*shutdown and retrieval*' and '*restoration*' receive the main focus. The system is initially in the working state, where the measurement uncertainty is 0.09%. When one USM is lost, the system reaches minor degradation state and the measurement uncertainty is increased to 0.11%. When two USMs are lost, the system reach the major degradation state and the measurement uncertainty is increased to 0.15%. When the system reaches this state, the maintenance event may be planned immediately (strategy I), or postponed with acceptance to operate under severe degradation (strategy II), or ignored, when in the later phase of operation (strategy III). This said, the condition for transition '*prepare for retrieval*' varies based on maintenance

strategies. When all USMs are lost, the system must shutdown and prepare for maintenance immediately. After maintenance, the faulty USM are replaced (i.e. as good as new) and metering station is restored to working operation state. The state diagrams for SEUs and jumpers can be established in the similar fashion, which are not illustrated here. It may be noted that state-diagram is one of many methods to complete design analysis. The same information can be obtained using flow-based diagrams such as FFBD and activity diagrams.

The physical attributes of USM assembly (e.g. dimensions, materials, component quality, manufacture process and locations) may impact the failure rate of equipment. For instance, the location of metering should be distant from control valves, as the noise of valve operation can interfere with USM measurement. Unfortunately, there lacks suitable data to evaluate such impact. In addition, the modularity issue is not critical for USM assembly since it is no such flexibility in maintenance according to the stakeholders' needs. In this case study, only physical decomposition is employed to assist FMECA construction in RAM analysis.

5.4.2 RAM Analysis

- **Dysfunctional analysis and failure rate predication**

Table 5-3 Part of FMECA for USM assembly

Unit	Failure mode	Failure mechanism	Failure rate (per 10^6 hours)
USM	Abnormal instrument reading	Changes in flow profiles, ultrasonic noise, high velocity (e.g. turbulence)	0.82
	Erratic output	Transducer failure, instrument or material failure	0.6
Jumper	Lose of connection	Water intrusion or loss of resistance	0.35
SEU	Control failure	Flawed control algorithm (fault signal/alarm), leakage, software failure	3
	Other types	-	1.05

FMECA is selected method for dysfunctional analysis since most of components are decided. Table 5-3 reports some failure modes of main equipment

on USM assembly. The failure rate for each failure mode given in the last column of Table 5-3, which is estimated based on the original data provided in the recognized database for subsea application OREDA [81] together with judgements from designer [114]. In this case study, only critical failures that lead to the loss of performance are taken into account, where the incipient failures or degradation are removed from scope.

- **RAM modelling and calculation**

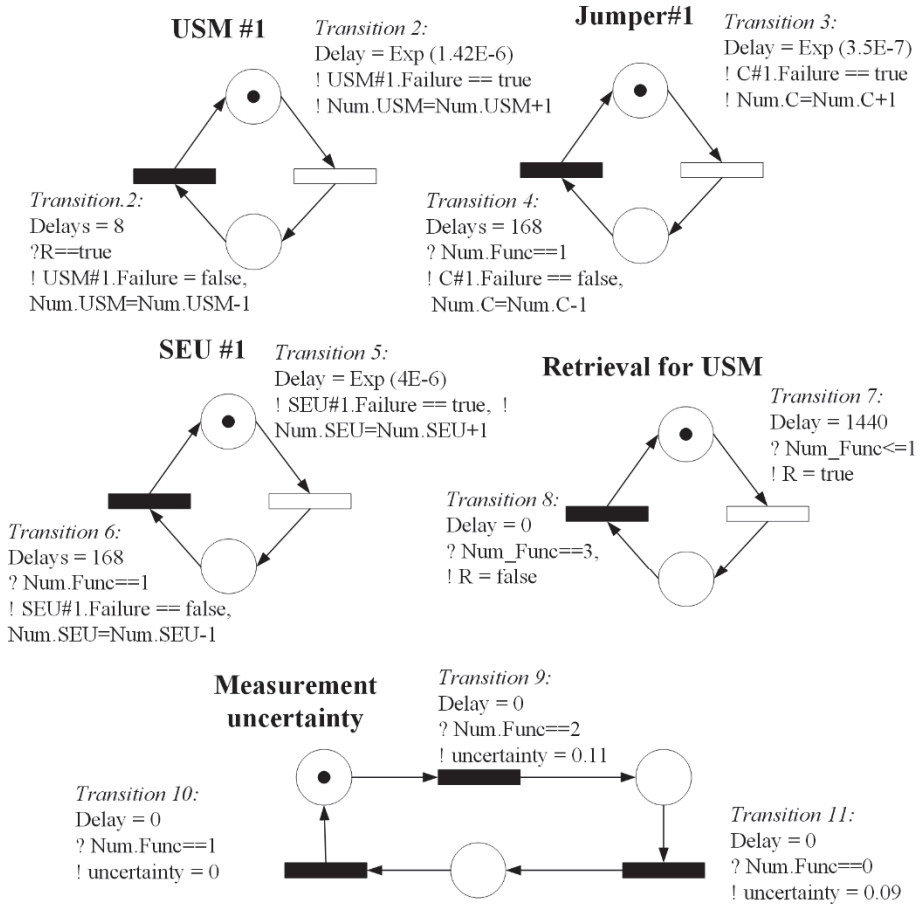
In this case study, SPN is selected for RAM modelling and calculation. Figure 5-10 presents part of SPN for case 1 (i.e. configuration 1 following strategy 1), where state-transitions in Figure 5-9 are mapping into Figure 5-10 by the *predicates* and *assertions* in the SPN. Predicate (represented by '?') is a formula to validate the transitions, and assertion (often represented by '!') is a formula to update the variables after the associated transition is fired [115]. The instruction for constructing Petri-nets model can be found in following articles [115, 116]. The synchronization of transitions indicates how each USM input is considered as valid or invalid given the states of USMs, jumpers and SEUs. The number of valid USM input is used to determine when to start maintenance and the uncertainty increment. For instance, case 1 following maintenance strategy 1 then the maintenance of USM assembly is planned when two valid USM inputs are lost. SPN model of case 2 to case 6 are constructed in the same way.

The computation for RAM modelling is completed by the software GRaphical Interface for reliability Forecasting (GRIF) [117]. The simulation run is set as 100000. The downtime and retrieval frequency of case 1-6 are reported in Table 5-4 and associated measurement uncertainties are illustrated in Figure 5-11.

On basis of both design analysis and operational analysis, the assumptions and constraints are made for RAM modelling as follows, and they are valid for all cases to be evaluated:

- For each USM, SEU and jumper only consider two states: faulty and working.
- The sensor lines are continuously checked, thus the delay for detecting failures on jumper and SEU can be ignored.
- All components are considered as good as new after maintenance. The activities of maintenance are considered as perfect thus no adverse effects are induced.
- Ideally, the subsea operator does not expect any retrieval during the operation until the metering system cannot perform the function as

intended (i.e. no redundancy has been planned for the USM assembly). Assuming that restoration duration ω =8 hours and mobilization time η= 1440 hours (i.e. two months), and the intervention will be carried out after 20 years of installation (i.e. 175200 hours).



Synchronization of transitions:

Func.1= 1 if USM1 is working and either jumper1 and jumper2 is working and either SEU1 and SEU2 is working, else 0

Func.2= 1 if USM2 is working and either jumper1 and jumper2 is working and either SEU1 and SEU2 is working, else 0

Func.3= 1 if USM3 is working and either jumper1 and jumper2 is working and either SEU1 and SEU2 is working, else 0

Num.Func=Func.1+Func.2+Func.3

Figure 5-10 SPN model for case 1

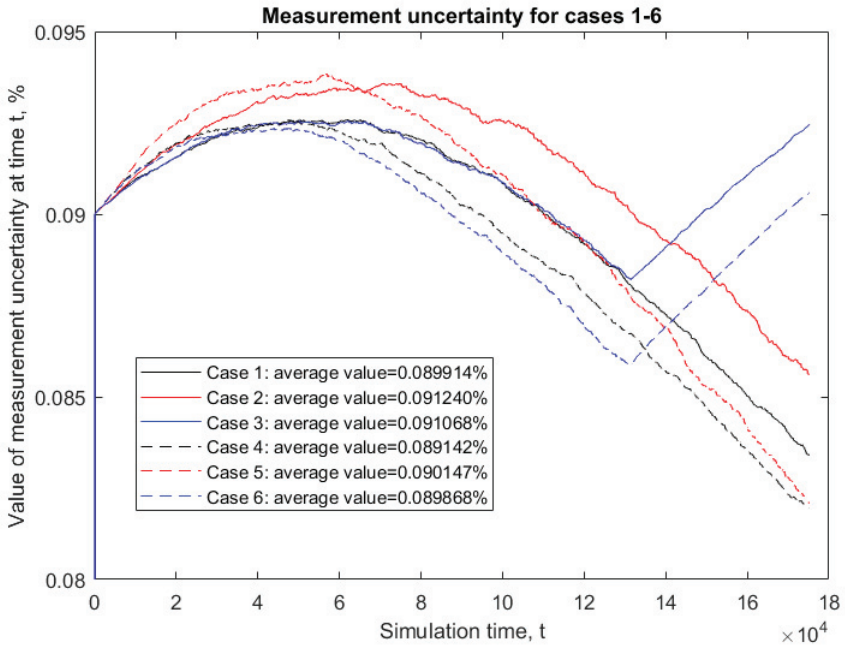


Figure 5-11 Measurement uncertainty for case 1-6

Table 5-4 Downtime and retrieval frequency for case 1-6

Case number	Expected downtime in 20 years (hours)	Expected retrieval frequency per 20 years
1 (configuration 1, strategy 1)	249	0.1733
2 (configuration 1, strategy 2)	225	0.1563
3 (configuration 1, strategy 3)	157	0.1092
4 (configuration 2, strategy 1)	418	0.2127
5 (configuration 2, strategy 2)	402	0.1988
6 (configuration 2, strategy 3)	391	0.1923

The indications from RAM modelling are derived as following:

- Table 5-4 contains the retrieval frequency of USM assembly and the downtime to replace jumper and SEU. As result, configuration 2 (case 4, 5 and 6) has much more downtime than configuration 1 (case 1, 2 and 3).

- Applying strategy 2 (case 2 and case 5) needs less maintenance than applying strategy 1 (case 1 and case 4) by paying the price of allowing an increase in measurement uncertainty.
- Applying strategy 3 (case 3 and case 6) results in the increment of measurement uncertainty in the last five years of lifetime (i.e. the turning points in Figure 5-11) as the system is allowed to operate with single USM. The downtime due to maintenance is significantly reduced compared to strategy 1 and 2 for configuration 1 (case 1 and case 2), however, not for configuration 2 (case 4 and case 5).
- Configuration 2 (case 4, 5 and 6) has more maintenance needs than configuration 1 (case 1, 2 and 3), and the maintenance need does not vary too much given the different maintenance strategies. As result, the measurement uncertainty is decreased.
- The peak value of measurement uncertainty for configuration 2 (case 4, 5 and 6) comes earlier than configuration 1 (case 1, 2 and 3). The reason is that configuration 2 loses flexibility as the SEU is not fully redundant for each USM.

5.4.3 Joint Concept Analysis and Communication

- **Design review and suggestions for re-assessment**

The major considerations derived from the selected analysis in RAM-SE framework are reported in Table 5-5. These considerations may either require designers to re-evaluate the system concept, or RAM analysts to re-construct the RAM model to achieve more realistic design implications. For example, the maintainability analysis shows that it is necessary to consider the separation between measurement instruments and sampling systems. Therefore, DSM is required for design analysis for mastering the interaction between these two modules and subsequent RAM analysis. Another example could be CCF assessment. The series connection of duty USM, master USM and spare USM can introduce the common mode errors due to the same design, installation and function. In this case study, common failure mode for USMs is mainly the deposits, e.g. wax. The designer indicated that the implemented measure is to heat the flow thus prevent wax formation [114]. Such communication should be documented and registered. If the related measure cannot be implemented given other design constraints (e.g. space and cost for heating strategy), then the effect of CCF should be incorporated in the calculation and modelling and the RAM analysis in subsection 5.4.2 will be updated to introduce the associated events.

Table 5-5 Considerations for USM design

Analysis	Key results and comments	Required follow-ups
Zonal analysis [19]	- The noise of control valves can influence USM performance - PT installed in the close location may cause the turbulences that influence USM performance	- Develop strategy and associated equipment to reduce the effect of noise if cost and space allows, e.g. noise trap or bends in piping. - Keep the necessary distance between PT and USM, e.g. at least 3 diameters of downstream [118] .
CCF assessment	- The series connection of USM offers better quality monitoring capacities but common mode errors of USM are introduced, which can influence the performance of USM and calibration process.	- Develop strategy for eliminating the potential factors on CCF, e.g. improve manufacturing process and upgrade on-site calibration process by taking CCF into account, see also the guideline in IEC 61508 [39].
Maintainability analysis [113]	- The sampling system has higher maintenance needs than metering module.	-The sampling system can be in a separate module to offer better RAM performance if cost and space allows.

- **Constraint-based decision making**

The constraint-based decision making, such as life cycle cost analysis, should be used to select the cost-effective alternatives for this design concept. The result of previous RAM analysis gives indications for two cost functions in life cycle analysis: the total cost for maintenance including resource mobilization and spare parts, and the profit loss due to system downtime and measurement uncertainty, where all the losses are converted into a monetary unit, i.e. Norwegian kroner (NOK). The selection criteria for costs functions and procedure of cost analysis can follow the existing standards such as NORSOK I-106 [119] or the internal procedure of the oil company. For instance, in this case study the net present value of oil in subsea storage is assumed as 2 hundred billion NOK and direct costs to replace the USM assembly is estimated as 25 million NOK. The result of cost analysis shows that case 1 saves the most. Compared to the most costly case 2, case 1 can save 4.03 million NOK in stakeholder's favor during the operation of 20 years, without considering the purchase order cost, project costs and technology development costs.

Communication plays an essential role in any engineering process as illustrated in the RAM-SE framework. What is meant by communication here is not documenting the numerical results that may fall into 'playing a number game' but *telling the story* under a consistent background. In this case study, by performing operational analysis and design analysis, RAM analysts can easily identify what is beyond the normal operations viewpoint and clarify the assumptions and simplifications for RAM modelling and calculation. The result of RAM analysis is thereby situated in a well-defined context to support the decision making in a design process. In this case study, by starting with operational analysis the issue to be investigated is specified: the impact of maintenance strategies and configurations. Design analysis identifies the functional and architectural aspects behind the issue: the system behavior (i.e. states and transitions) of selected configurations under different maintenance strategies. The information can be used to construct a RAM model and the numerical results through simulation can be used for selection of design alternatives. It is important to remember that the using RAM-SE framework is never to prove that models are close to the reality but to ensure RAM analysis are illuminating and useful to consider the design implications when the context is defined properly.

5.5 Discussion

It has become apparent that incorporating RAM aspects as early as possible gives several advantages in form of engineering efforts and budgets. Many companies involved in subsea development have their procedures for framing RAM in design but they still claim that they are not adequate. The similar problem already exists in many industry sectors such as nuclear, satellite and aviation, where the problem is further amplified by the complexity of design solutions. This work selects subsea design as the starting point. Analysts in this context, often dive into RAM analysis before correctly stating the system concept. Development of a system concept by RAM techniques relies on competence, experience and the knowledge base of analysts, which often results in inconsistency and misunderstandings. Without a more holistic framing, RAM in subsea design has limited possibility to give systematic insight of the design concept, making it necessary to integrate other disciplines to complete industry practice.

The proposed RAM-SE framework discloses the link between the RAM discipline and SE discipline, by connecting the concepts and models used by these two disciplines. Yet, the case study here provides a rather 'crude' RAM analysis according to RAM-SE framework, where only the critical steps and selected results are presented. The details procedures of RAM analysis itself, for example about how to complete dysfunctional analysis, are not presented in this chapter.

It is therefore hard to discuss the practical values of RAM-SE framework at this stage. The following four chapters are dedicated to propose the new models or discuss the required knowledge to support the domain of RAM analysis. The evaluation of RAM-SE framework is therefore presented afterwards in Chapter 10.

Chapter 6 STPA for dysfunctional analysis

Subsea systems become increasingly intelligent and more dependent on software, so understanding the dysfunctional behavior associated with the issues of properly controlling such systems is needed. Unfortunately, many of the traditional methods for dysfunctional analysis are not adequate for this purpose. Instead, a new hazard identification method named STPA recognized as a promising candidate [120]. Yet, there is no guideline for utilizing STPA output in reliability modelling to evaluate the potential of loss, which is important for basis for decision-making about system configuration and equipment selection.

This chapter firstly gives an overview on dysfunctional analysis, which indicates why STPA is needed, followed by the introduction of the original STPA to summarize its advances and shortcomings. Afterwards, a step-wise approach is proposed for developing the STPA-RAM model that extends the application of STPA. The main idea is to translate hazard scenarios obtained by STPA into SPN for discrete event simulation. Finally, SGB is selected as an illustrative case to demonstrate the applicability of STPA-RAM model and discuss its usefulness and further improvements.

The main content of this chapter is based on the submitted article [121] prepared as part of this PhD project, see the appendices for original content.

6.1 Dysfunctional analysis

Dysfunctional analysis is an important step to verify that the system is able to operate according to specifications under different operating conditions. It helps to create a consistent understanding about how a system lose its functions (further dissatisfy the defined requirements) due to the nature of a system, its environmental stress and harmful interactions. Dysfunctional analysis may in this sense to aware the weakness of design and not be simply seen as opposite of functional analysis.

Studying the mechanism, causes, criticality, and other attributes of dysfunctional behavior is the central element of analysis. The dysfunctional behavior can be the subject of different analyses, for instance *failure* in RAM analysis and *hazard* in risk analysis, where these two terms are not simply equated to each other [122]. Failure is generally defined as the termination of performing required function [12]. Hazard has abundant definitions from literature (e.g. [123], [79] and [124]), but the common understanding of this word pointing to two aspects: (1) a condition or a set of circumstance, (2) potential/source to unwanted events. For the purpose of identifying dysfunctional behavior, it is not

essential for such distinction on failure or hazard. To avoid the possible ambiguity, hereby a rather board definition of *failure* (as it is more commonly used in the RAM domain) is proposed:

'*Failure is the (fully or partial) loss of intended functions that achieve values to stakeholder*'.

This definition grasps the main features of two terms. The first part of the definition is based on functional perspective but emphasizes on *loss* instead of *termination*. The second part of the definition emphasizes a wide range of unwanted events/losses, covering from typical concerns of risk analysis (e.g. human injury, property damage, and environmental pollution) and mission concerns of RAM analysis (e.g. mission loss and economic loss).

6.1.1 Failure classification

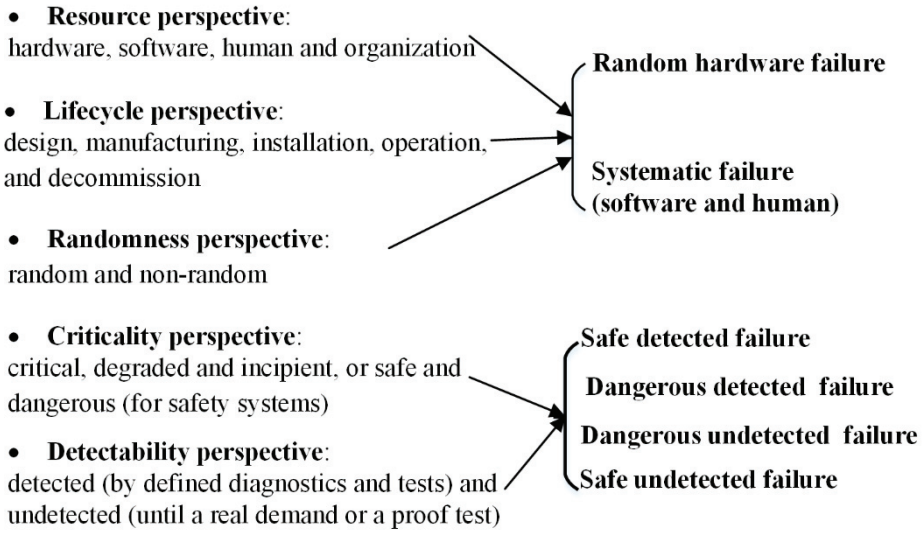


Figure 6-1 Commonly-used perspectives for failure classification

Figure 6-1 illustrates several commonly used perspectives for failure classification. IEC 61508 [39] distinguishes between *random hardware failures* and *systematic failure*, given the first three perspectives. Random hardware failure, as the name already says, is a failure caused by one or more degradation mechanism (e.g. aging) and occurs at a *random* time in the *hardware*. Systematic failure can happen whenever the premise condition is satisfied [64]. It could be introduced in any lifecycle of system and seen as complementary set to random hardware failure, includes software failure, design and installation related failure,

and human errors during operation and maintenance. This classification is used to set the correct scope of RAM modelling: only random hardware failure is considered for quantification, whereas the impact of systematic failure is negligible as it must be corrected by modification of design and manufacturing [39]. In this respect, failure originating normally software and human draw little attention in RAM modelling. Although this classification is well-argued in a highly recognized standard, some adaptions under specific context may be needed. One example is human-related failure. As argued by ISO/TR 12489 [9], failures induced by human-triggered interaction (e.g. routine operation and maintenance) can be assumed as random, whereas only human-related failure induced by social factors (e.g. insufficient training and improper human machine interface) are considered as systematic failure. The discussion on this issue is continued after presenting the case study, where human and software are used to implement system control.

Classification based on criticality is used data collection and analysis practices (e.g. OREDA [81] and ISO14224 [125]), as the criticality is key indicator rank the severity of failures. The *criticality* here refers to whether the item has the ability to perform its essential function. For instance, the critical failure means that the item *totally* loses its ability to perform function on demand or maintain the production. Degraded failure implies that the item has degraded performance but still perform the essential function in an acceptable way. The incipient failure (or partial failure preferred by some) refers to the situation that degradation is under development. For safety system, criticality simply concerns whether the system safety is compromised or not by the failure, so there are only *safe* and *dangerous* failure. The classification of detectability of failure is more precisely defined in Appendix B of ISO/TR 12489 [9], by linking the efficiency of diagnostic and periodic test (or more generally the testability). The classification based on these two perspectives are adopted in the part 4 of IEC 61508 [39] and PDS method [126], which can be seen as supplement to previous classification to derive the definition of corresponding failure rates and assumptions for reliability modelling and assumption.

The failure classification schemes presented above focus on individual part of a system, where failure occurrence is assumed as independent event. Another critical factor is Common Cause Failure (CCF), which receives attention in particular nuclear industry as it limits the expected reliability improvement from redundancy [127]. CCF is defined as '*the failure that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system*' [39]. Hauge et al. [128] stated that it is difficult to argue CCF is entirely belongs to random hardware failure or systematic failure, but it is often *caused* by systematic failure. Generally, the cause of CCF can be

categorized into root cause and coupling factor [64]. A root cause is a basic cause like extreme environment condition (e.g. bad weather and ultra-deep water). A coupling factor reveals that failures of components caused by the same root cause (e.g. same design and same maintenance) [129]. The commonly used methods for CCF modelling are beta-factor model, binomial failure rate model and multiple beta factor model, see e.g. [106] for a brief summary. In addition, the defense approach is also needed to improve awareness of CCF, reveal CCF causes and design measures against CCF. In O&G industry, some initiatives have already been taken. Hauge et al. [128] have utilized field experience to form a checklist to update beta-factors in CCF modelling. Lundteigen and Rausand [129] have discussed how to integrate CCF defense approach with existing practices like function test and inspection.

The failure classification serves as the first step of dysfunctional analysis and decides its scope. That is, the failure not classified into any category is no longer considered in a dysfunctional analysis. In this respect, a proper failure classification relates to the *coverage* of failure identification discussed in next subsection.

6.1.2 Failure identification

Failure identification is crucial for looking for when and how to execute the mediating measures for designing RAM into product. Some well-known models for this purpose are reported in Table 6-1.

Table 6-1 Commonly-used models for failure identification

Methods	Description	Constraint
FMECA	- reveal failure modes and causes of individual items and guide the risk reduction work	- unable to identify the sequential and combinatorial property of failures
HAZOP	- identify the hazard potential of operation (as supplement to failure modes of items)	- requires experienced personnel and detailed information about systems (which implies it not applicable in early phase of design) [15, 59]
FTA	- retrospective analysis for identified hazards - smooth transition to quantitative modelling	- not applicable for revealing hazards on early stage -strictly assuming the independency between items
SWIFT	- feasible and easy method to be implemented into practice	- being experienced facilitator dependent

Among that reported in Table 6-1, FMECA and HAZOP are widely used in both industry and academia. There has been several improvements for FMECA and HAZOP to improve their effectiveness of analysis procedure and applicability, see, e.g.[130] [131]. In addition, FMECA and HAZOP bear strong similarities, whilst they entail independency. Compared to FMECA that focuses on distinct components, HAZOP is rather function-driven and focuses on production on the consequences of deviations related to process parameters. Some initiatives have been taken to combine the advantages of FMECA and HAZOP, see e.g. the integrated approach proposed by Giardina and Morale [132] and Blended Hazard Identification (BLHAZID) method proposed by Seligmann et al. [133].

The traditional models for dysfunctional analysis are argued to be challenging for subsea system built today. The challenge may be attributed to the deficiencies in modelling complexity, as well as the lack of knowledge about the system to study in early design phase. First, when applying FMECA or HAZOP, components and operating procedures are analyzed individually, and the interaction within are analyzed pairwise, thus the combined effects of failures are not properly covered. Second, some traditional model like FMECA is essentially bottom up approach based a hierarchical view. In this regard, it cannot be carried out in early phase where the components have not been settled yet.

Some candidate models have been proposed by researchers, such as Accimap [134], Functional Resonance Analysis Method (FRAM) [135] and Systems Theoretic Process Analysis (STPA) [80]. Of the mentioned methods, STPA is the approach that has gotten the most recent attention in this thesis due to its suitability to analyze software-intensive systems. It has been applied with reported success in different applications such as automotive [136], healthcare [137], aerospace [138] and subsea [120, 139]. As a hazard identification method, STPA can be naturally embedded in safety and security analysis [140, 141] by guiding the associated controls and mitigating measures depending on different applications [137, 142, 143]. Some of the advantages and examples of applications of STPA could be found in literature [120, 144, 145]. So far, the commonality and acceptance of STPA is delimited to the academic circle as it has not standardized basis. Yet, it seems very promising to use STPA as complementary to FMECA and HAZOP to efficiently increase the coverage of dysfunctional analysis [145]. To evaluate the applicability STPA in RAM analysis, some familiarization with the model itself is needed. That is the task of next section.

6.2 Introduction to STPA

6.2.1 STPA procedure

The practical execution of STPA is led by STPA analysts, i.e. persons with good knowledge in STPA analysis, and involves system experts to ensure the deep knowledge of design and engineering issues. It is not always reported in papers on the application of STPA if the analysis takes place as a workshop session with all involved persons present at the same time, or if the analysis is carried out during a sequence of meetings where persons are consulted as needed. In practice, there may be examples of both approaches.

STPA has been under continuous development since emergence, and its framework can be complicated with respect to the analytical needs and constraints for practical use, e.g. [146]. This section follows the generic steps suggested in STPA handbook by Leveson and Thomas [80], which are illustrated in Figure 6-2.

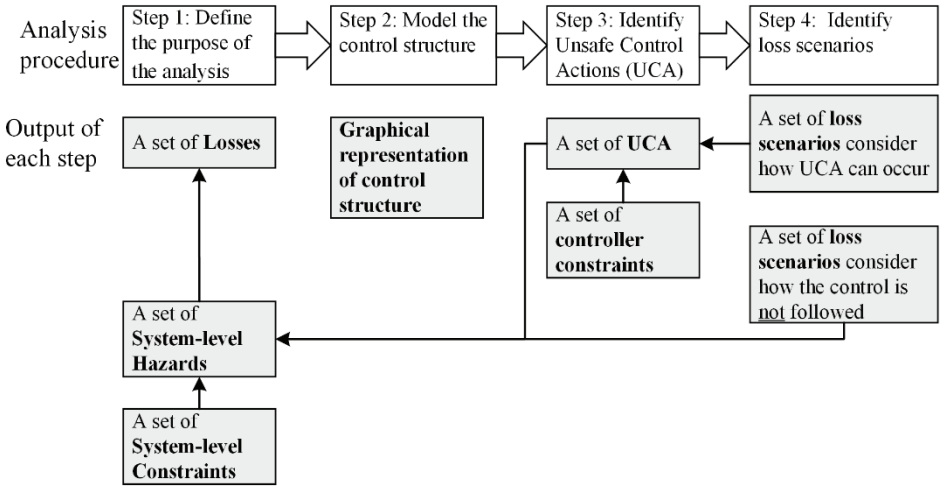


Figure 6-2 The framework of STPA and its output

- **Step 1: Define the purpose of analysis.** The first step is to define the scope of analysis by identifying the consequences on system level in presence of any single or multiple variations on feedback control loop. The consequence includes the losses and associated hazards. *Losses* could be any type of dissatisfactory value to stakeholder when the system fails to achieve its goal and objective, and system-level *hazards* are a set of system states that can lead to losses together with worst-

case conditions. Such broad definition of losses and hazards implies that STPA covers traditional safety issues as well as RAM issues.

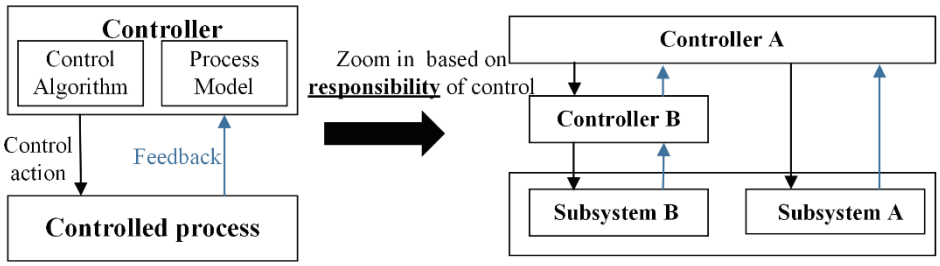


Figure 6-3 Example feedback control loop

- **Step 2: Model the control structure.** The next step is to develop the hierarchical control structure of a system, which consists of one or more feedback control loops. A feedback control loop is a graphical representation, which involves all the elements that have impacts on the emergent system properties in form of their individual behavior and interactions. An example of a feedback control loop is illustrated Figure 6-3, from the left to right the details are added based on the responsibilities assigned to each element. The hierarchical control structure can be refined until the suitable granularity is reached, to have the global and complete vision about the hierarchy concern being controlled, thus supports the following step 3 and step 4.
- **Step 3: Identify Unsafe Control Actions (UCAs).** The third step relies on the structured identification of what can go wrong, using the feedback control loop and a prepared context table as basis. The output of this step is a list of UCA that in particular context results in one or more of the hazards identified in step 1. The UCAs are be identified through four guide conditions taking advantage of control structure: (1) the control action is not provided, (2) the unsafe control action is provided, (3) control action is provided too late, too early, or out of sequence and (4) control action is stopped too soon or applied too long (applied only for continuous control). The constraints for controller can be defined as conditions or behaviors to prevent occurrence of UCAs (and ultimately prevent related hazards).
- **Step 4: Identify loss scenarios.** Loss scenarios are used to describe the casual factors that lead to hazards (and ultimately to losses in worst-condition). The first type of loss scenarios consider how the UCA can occur, including the causes of unsafe controller behavior and inadequate feedback. The second type of loss scenario consider how the safe control action is not followed, including the causes of deviated

control path and controlled process. The control structure obtained through step 2 need further refinement by including the sensors and actuator of the control loops so that analysts can examine why the feedback is not detected or wrongly detected and why the control action is not followed or improperly followed by actuators.

The new insight brought by STPA is the characterization of erroneous or inappropriate control and associated causality knowledge. All elements of a system (i.e. hardware, software, human and organizational factors) are considered as the contributors (i.e. controller and controlled process) in the feedback control loop. The loss scenarios are therefore determined when the *combination of* control commands, inadequate feedback, and the state of the controlled process and its environment is inadequate or improper. Such systematic way of hazard identification goes beyond the scope of traditional methods based on the common engineering sense (i.e. hardware-wise). In this respect, STPA is suitable for analyzing subsea system built today, which becomes increasingly intelligent and more dependent on software.

While STPA provides an alternative model for hazard identification and theoretically increases the coverage of failure identification, the current framework of STPA strictly emphasizes on qualitative aspects and has no guidance on how to direct the further quantification. In such set-up, STPA has no guidance on how to direct the further quantification of loss scenarios, which leaves designers with challenging tasks to interpret STPA results in the decision making. Few attempts have been made to systematically use STPA outputs to improve RAM modelling, whereas a similar link can be readily found for traditional models, e.g. FMECA and HAZOP. The lack of this connection is unfortunate as important insight can be overlooked and not transferred from STPA to RAM modelling. This is also pointed out by Hafver et al. [147], who suggest that the STPA output has the potential to construct better RAM modelling to predict the effect of improper/inadequate controls on system behavior. Yet, the architect of STPA, Leveson [79] has argued that quantitative analysis in STPA is questionable, for mainly two reasons. First, pursuing quantitative analysis can distract the attention away from important causal factors that are not characterized statistically [122]. Second, it requires probabilistic insights about future events that are not supported by historical data. Assigning probabilistic information for loss scenarios is a challenging and error-prone task even with excessive elaborations among system designers and experts.

Yet, for high-risk industry like subsea, such *deterministic* approach is not adequate to convince the operators that the product is fit-for-use. It is difficult to eliminate all possible loss scenarios in reality as countermeasures may degrade or become less efficient over time, see examples in [143, 144] where STPA is

applied to technical system. It is therefore necessary to evaluate the effect of loss scenarios that have not been observed yet versus considerable costs for provision of countermeasures. The lack of probabilistic data does not mean the *probabilistic* model is useless in the context of STPA. The probabilistic model can provide in-depth assessment to address risks induced by, and anchor STPA results in the engineering decision context.

In a short summary, original STPA has both advantages and inadequacies. Although STPA reveals a full spectrum of vulnerable points for given design concept, it leaves all judgments about prioritization of design improvements and modifications to the designers. The effect of designed countermeasures may not be obvious without constructing quantification model. Stimulating how the system responses to perturbations on feedback control loop through a defined mathematical framework can be a solution to this problem. That is the topic of next section.

6.2.2 Theoretical basis for simulation

According to Thomas [148], an UCA (and its descendant – loss scenarios) can be defined with a formal structure as a quadruple <***Ac***, ***CA***, ***Co, U***>, where:

- ***Ac*** is a set of actors refer to at least one controller of the controlled process.
- ***CA*** is a set of control commands issued by controller Ac ∈ ***Ac***.
- ***Co*** is a set of contexts that defines a unique system state, which implies whether the control action is needed (given) or not. ***Co*** can be specified explicitly or implicitly in terms of distinct variables. Each Co for the controller Ac should be independent.
- ***U*** is a set of hazardous state (i.e. description of possible and relevant losses). To be qualified as UCA, a control action must satisfy the property that (Ac, CA, Co) can lead to at least one of U ∈ ***U***

A control process can be equivalently transferred into Finite State Automata (FSA). FSA is used to model the discrete behavior of system, consists of a finite number of state, transitions between states and events. The *state* represents a quiescent node in the sequence of a control process, and the *event* describes the control action to be performed. A control-like *transition* triggered by an event or condition can cause the change of state. For instance, if providing a control action under a specific context that causes hazards, the transition function is $\boldsymbol{T}$: $\boldsymbol{Co} \times \boldsymbol{CA} \rightarrow \boldsymbol{U}$. In this sense, the system in question is reformulated as the closed-loop

control where the feedback signals (i.e. state of system) are now being used to both control and adjust itself.

The change of states (i.e. ***Co***) is modelled by random and deterministic events defined for a system. RAM model is one example, in which the failure and degradation are considered as stochastic events and software updates and hardware replacement are considered as deterministic. Therefore, one can establish the interface between RAM modelling and loss scenarios derived by STPA through FSA. The effect of loss scenarios on RAM performance can be simulated by FSA under the following assumptions: The transitions between states describe the situation where the control actions (no matter safe or unsafe) update values of model parameters (e.g. failure rate) in the new state. The changes made for model parameters influence the related transitions in FSA as a function of time. For example, a shutdown valve may be exposed to the hard stress in the situation of 'slam shut' closure, which can be seen as a loss scenario and its consequence is the permanent damage on valve. This implies the accelerated degradation rate for the shutdown valve once reaching the hazardous state that defines above situation.

6.3 Proposal: STPA-RAM modelling

Given the settings defined above, this section presents the proposal named STPA-RAM modelling. SPN is selected as the suitable modelling approach that follows state transition formalism.

6.3.1 Two-steps approach

Figure 6-4 illustrates the two-steps approach: The first step is to carry out an STPA to identify loss scenarios. The second step has to main sub-tasks: (i) to prepare RAM model using available specifications for the system and its intended functions, and (ii) to complement this model with new information from STPA in the first step. The outcome is a revised RAM model representing new information about dependencies in the feedback control loop developed by the STPA, namely a STPA-RAM modelling.

In the approach, the STPA-RAM modelling can reflect the potential deviations in different feedback control loops and interfaces between feedback control loops. Causality knowledge obtained in STPA is maintained in the STPA-RAM modelling. The loss scenarios can be generated by studying the reachability to the hazardous states. The actors of feedback control loops (i.e. hardware, software and organizational factors including human) are closely tied together in FSA in which the interdependencies between feedback control loops are represented by transitions. To maintain in the same format for integration, RAM modelling is

constructed as the feedback control loop. In this regard, the monitoring and inspection on the state of controlled process are the considered as the feedback loop to the maintenance and intervention controller, whose responsibility is to update the software or replace the hardware when the feedback indicates the malfunctions and deviations of controlled process. Such modelling approach goes beyond the classical RAM modelling that is built on propagating the information from low-level system hierarchy along with simple logics.

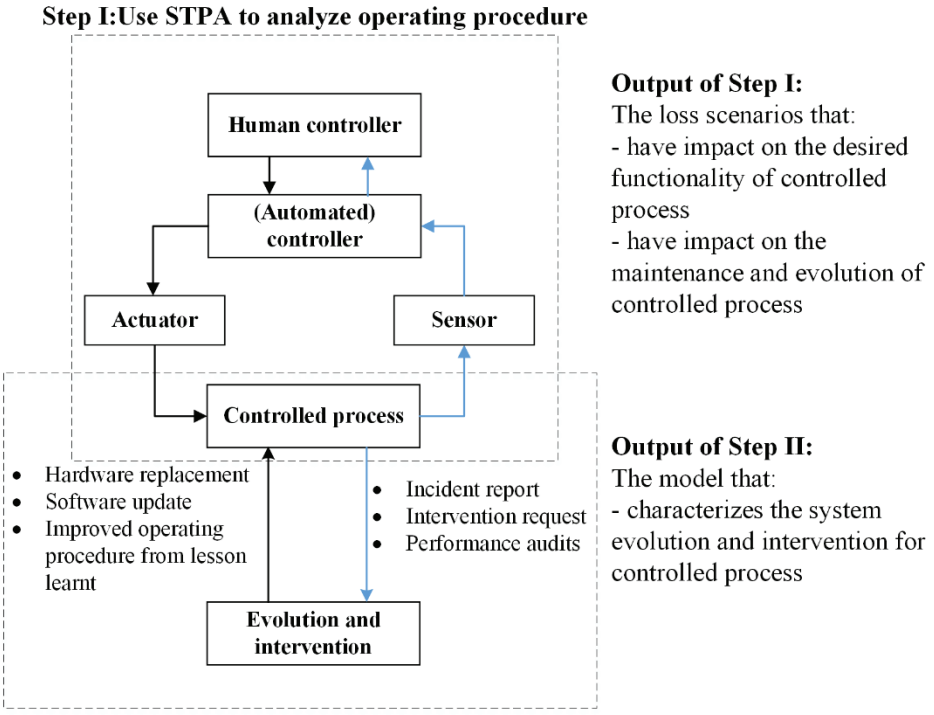


Figure 6-4 Two-steps approach for STPA-RAM modelling

The proposed approach covers multiple models and the coordination between models are rather complex. The complexity here depends on the number of feedback control loops. The original feedback control loop defined in STPA is inadequate to express such complex coordination and has no execution ability. SPN that follow the state-event transition formalism is selected to structure models of proposed approach, without distorting the feedback control phenomenon of STPA. It may be noted that SPN is only one of many ways to visualize such interactions and construct the executable model. The other methods obeying state-transition formalism can achieve the same objective but they are not further discussed in this chapter.

6.3.2 Use SPN to construct STPA-RAM model

The SPN model consists of a *net structure* and a *marking* [149]. The net structure is made of the *places* (represented by circle), *transitions* (represented by bars), and their connection (presented by directed arcs). The arc links a place to a transition is called input arc and the arc links a transition to a place is called output arc, and they can be assigned with a natural number, named *weight* or *multiplicity* (normally assumed to be 1). Places may contain *tokens* (represented by bullet), which can move between places when enabled transition is fired. The transition is enabled when a number of token on each of its upstream places (a place connected by input arc) is not less than the weight/multiplicity of input arc. The transition is fired when the associated delay elapses (given that transition remain enabled during delays). The time delay between enabled transition and firing can be characterized as fixed or random [150]. The marking represents the distribution of tokens on a net structure. In such setting, the place of SPN can specify the context as premise condition for control action, and the tokens specify the state/value of context that decides whether the control action is needed or not. The transitions represent the control actions and information feedback on feedback control loop, and the time-dimension of control process is introduced by the random or fixed delays. In addition, *predicates* and *assertions* by means of variables can be introduced to SPN [115]. Predicate (often represented by '?') is a formula to validate/disable the transitions when variables are verified/unverified, and assertion (often represented by '!') is a formula to update the variables after the associated transition is fired. The predicates can model synchronization between control actions and controlled process, and the assertion is used to capture the transformational change in the system as the result of executed control actions. The detailed information about how to construct SPN model can be found in [115, 116]. The rest of this section introduces a small example for using SPN to construct STPA-RAM modelling.

Figure 6-5 illustrates an example feedback control loop represented by SPN model. Two piecewise SPN models are structured to represent the behavior of controller and controlled process. The controlled process (i.e. system) can become abnormal and this is assumed as a stochastic process. The responsibility of controller is to intervene with the controlled process when it is in abnormal state, and system state is either maintained or, when relevant, reset to normal within the permitted time (X seconds). The two variables considered for predicates and assertions here are denoted as *normal_state* and *reset*.

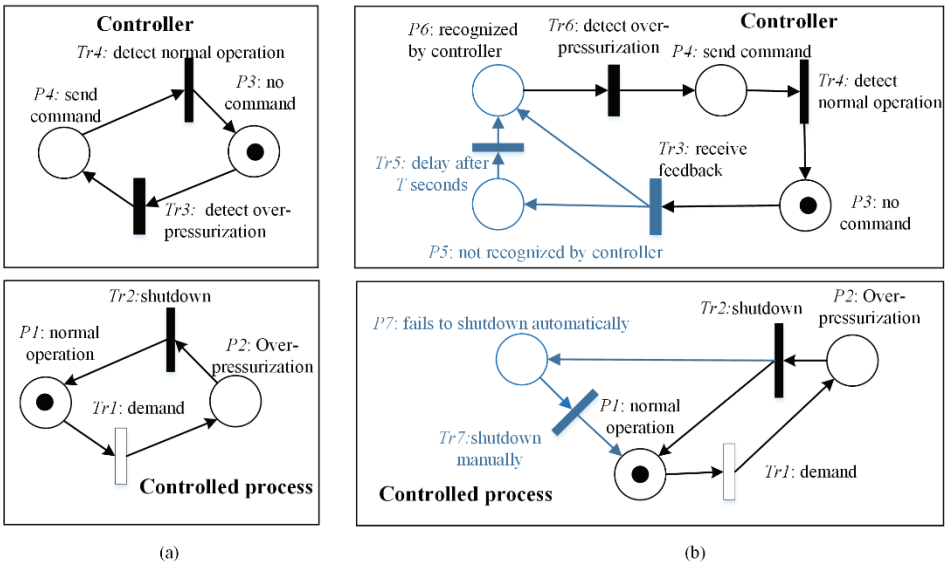


Figure 6-5 SPN models for (a) adequate control (b) two potential loss scenarios

Figure 6-5 (a) illustrates SPN model for the defined feedback control loop, assuming there is no loss scenario as the result of adequate control. The tokens initially stay in *P1* and *P3*, representing the state that the system is normal so no need to intervene the system. The initial marking is that one token stays in *P1* and one token stays in *P3*, indicating that normal state of system and no control command. When the token reaches *P2* from *P1* after firing the transition *Tr1* (i.e. system state becomes abnormal), the assertion of *Tr1* is '! *normal_state* =false'. Then, the transition *Tr3* is fired as the predicate of *Tr3* is '? *normal_state* =false', means that the controller sends the command to activate the system when abnormal state is detected (by controller). Similarly, when the token reaches *P4* through transition *Tr3*, the variable *reset* is assigned as *true* to fire the transition *Tr2* (i.e. send command to reset the system/controlled process). When the token leaves from *P2* to *P1* (means the activate process is completed after certain delay), the variable *normal_state* is updated as true so that transition *Tr4* can be fired. Figure 6-5 illustrates an example feedback control loop represented by SPN model. Two piecewise SPN models are structured to represent the behavior of controller and controlled process. The controlled process (i.e. system) can become abnormal and this is assumed as a stochastic process. The responsibility of controller is to intervene with the controlled process when it is in abnormal state, and system state is either maintained or, when relevant, reset to normal within the permitted time (*X* seconds). The two variables considered for predicates and assertions here are denoted as *normal_state* and *reset*. Table 6-2 summarizes the synchronized product for Figure 6-5 (a).

Table 6-2 Synchronized product of case in Figure 6-5 (a)

Transition	Predicate	Assentation	Delay of transition
Tr1		normal_state=false	Stochastic delay, λ
Tr2	reset =true	normal_state =true	*X* seconds
Tr3	normal_state =false	reset =true	0
Tr4	normal_state =true	reset =false	0

Figure 6-5 (b) illustrates how the influence of STPA output is modelled in SPN where two loss scenarios have been selected, and they are represented by net structure colored as blue. Loss scenario 1 is that controller sends the command too late (after *T* seconds) when abnormal state is detected, which leads to the hazard denoted as H.1. In this case, the transition *Tr3* in Figure 6-5 (a) is divided to two transitions *Tr3* and *Tr6* in Figure 6-5 (b) to distinguish between the event 'receive feedback of state' and the event 'abnormal system state has been recognized (by controller)'. In addition, two new places *P5* and *P6* are introduced to represent the context that 'feedback has been recognized too late' and 'feedback has been recognized immediately' respectively. The loss for H.1 is expressed as the extra T seconds that system is exposed to the abnormal state, equals to the delay of transition *Tr5*. Loss scenario 2 is that system is not successfully activated in response to the command and that a manual reset (intended to compensate) leads to hazard denoted as H.2. In this case, the transition *Tr2* in Figure 6-5 (a) is divided to two transitions *Tr2* and *Tr7* in Figure 6-5 (b) to distinguish between the event 'reset system upon control command' and the event 'reset system manually'. The new place *P7* is introduced to represent the state that 'the system fails reset automatically'. The associated loss for H.2 is that the system is exposed to more stress when it is manually activated then the system is more prone to be abnormal in the rest of operation, saying that the transition rate of *Tr1* is slightly increased by α% after the transition of *Tr7*. The transition *Tr2* now has two downstream places: *P7* and *P1*. The frequency of loss scenario 2 can be denoted as the probability that token from *P2* enters into *P7* when transition *Tr2* is validated, that is '? *reset* =true'. Similarly, the frequency of loss scenario 1 can be denoted as the probability that token from *P3* enters into *P5* when transition *Tr3* is validated, that is '? *normal_state* =false'. Table 6-3 summarizes the synchronized product for Figure 6-5 (b).

Table 6-3 Synchronized product of case in Figure 6-5 (b)

Transition	Predicate	Assentation	Delay of transition
Tr1		normal_state=false	Stochastic delay, λ
Tr2	reset =true	normal_state =true	*X* seconds
Tr3	normal_state =false		0
Tr4	normal_state =true	reset =false	0
Tr5			*T* seconds
Tr6		reset =true	0
Tr7		$\lambda = \lambda \times (1+\alpha)$	0

Although a quite simple and restrictive case is considered in Figure 6-5, the above example is sufficient to illustrate how to construct STPA-RAM modelling by using SPN. One specific issue is the refinement of SPN. The SPN model in Figure 6-5 could be further refined by including SPN that represent sensor and actuator in the same feedback control loop or other actors from different feedback control loops. The coordination between actors are realized by the variables that are updated by assertion and propagated in feedback control loop by predicates. For instance, if the controller wrongly believes that the system is in abnormal state, a possible cause can be that the sensor provides the wrong feedback of actual state of system. To model this casual factor, one may construct another piecewise SPN that represent the evolution of sensor performance, e.g. *state_sensor*. The predicate of transition *Tr3* is subjected to the variable *normal_state* and *state_sensor*. The detailed example is given in the case study that follows in the next chapter.

6.4 Case study: subsea gate box

This section is to construct STPA-RAM modelling for SGB. Rather than focusing on the entire SGB concept, this case study is to study the unavailability and production deficiency caused by improper interactions between functional modules of SGB. The simplification is therefore made on the original design concept presented in 2.3. Same as the case study of Chapter 5 the modelling and simulation of SPN is completed by GRIF.

6.4.1 System description

Figure 6-6 presents one alternative configuration for SGB, where each SGB consists of three functional modules: separation module (SPM), choke valve module (CVM) and multiphase pump module (MPM). The normal processing line consists of SPM and MPM, where hydrocarbon flow is separated by separation unit into liquid and gas, where the liquid is pumped through multiphase pump and the gas is assumed to flow naturally to the manifold. When the functional modules of the normal processing are faulty, the hydrocarbon can be bypassed to CVM on the same SGB. The choke valve then controls hydrocarbon pressure with low production efficiency. A subsea control system that interacts with the SGB equipment and sensors is vital for maintaining an optimal operation. The switch between processing lines is controlled by subsea controller (s) and realized by the open/close of crossover valve (XOV). SPM, MPM and CVM are retrievable. The connection between module (e.g. isolation valves and pipe connectors) and the sensors (e.g. transmitters of flow, temperature and pressure) are not illustrated in Figure 6-6.

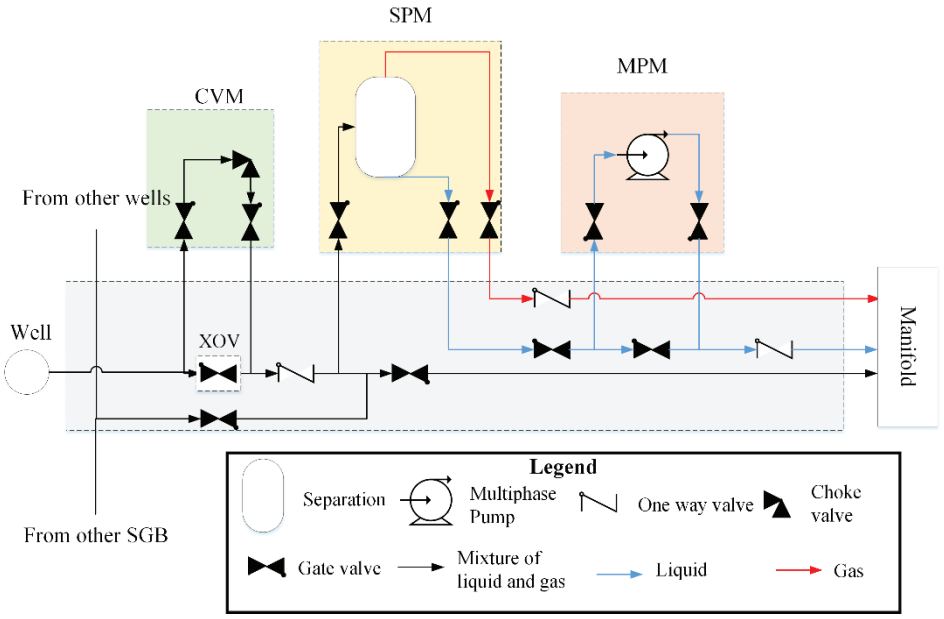


Figure 6-6 System schematic drawing of SGB

In the following subsections, STPA-RAM modelling is conducted for illustrative purpose. The first step is to carry out STPA for analyzing the operating procedure of SGB. The involved actors for the control action are simplified as normal processing line (SGB-NP), bypass processing line (SGB-BP), XOV,

sensor and controller. The second step is to build up RAM model considering the state of actors. Some data for RAM modelling are assumed for demonstrating the approach only. Given the numerical results obtained through STPA-RAM modelling, the countermeasures for selected loss scenarios are suggested. The selection of countermeasures are not discussed as the cost information for suggested measures are not available currently.

6.4.2 Step I: carry out an original STPA

Based on the discussion with the system designer, three types of losses were identified: unexpected decrease in production efficiency (L.1), hydrocarbon spills (L.2), and complete shutdown of SGB (L.3). The associated system level hazards and associated constraints are summarized in Table 6-4.

Table 6-4 System-level hazards and constraints

System level hazard (SH)	System-level constraints (SC)
SH.1: Hydrocarbons flow into non-optimal processing line [L.1]	SC.1 Hydrocarbons must always flow into optimal processing line
SH.2: Hydrocarbons flow into unavailable processing line [L.1, L.2, L.3]	SC.2 Hydrocarbons must never flow into unavailable processing line
SH.3: Over-pressurization of equipment in selected processing line [L.2, L.3]	SC.3 Pressure must never be built-up above design limit

The high-level hierarchical control structure is illustrated in Figure 6-7. The subsea controller consists of process control system (PCS), subsea control unit (SCU), process shutdown (PSD) system, SCM and SEM. The structure and complexity of subsea controller depend on the operating strategies and distance to controlled equipment [139]. For instance, PCS and PSD located on surface facility deliver the command from human operator to control equipment and shut down the system, through SCU to the SCM/SEM that located subsea. To simplify the case study, only SCM and SEM are considered, and the responsibility is distribute the control commands to equipment. When the ability to use the normal processing line is lost, human operator sends the coded command to SCM/SEM that distributes the command to associated valves. The SGB-NP is shut down by the closure of isolation valve, and XOV is opened thus the hydrocarbon is redirected to CVM with lower production efficiency. When the normal processing line is restored after maintenance, then human operator sends the command through the similar process to restart SPM and MPM and redirect flow to normal processing line.

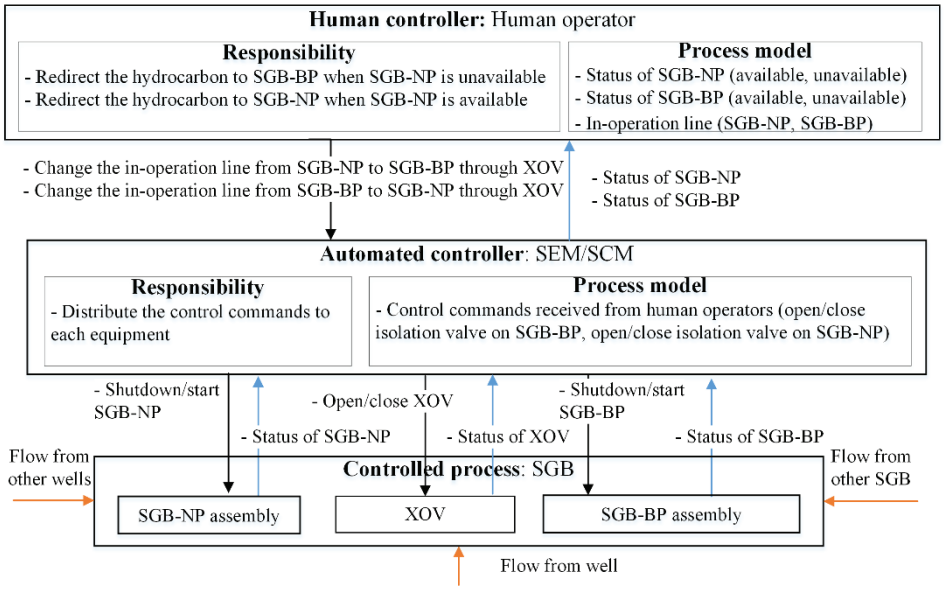


Figure 6-7 High-level control structure for SGB

Table 6-5 presents the example UCAs, given the high-level control structure of SGB.

Table 6-5 UCAs for defined control structure

	Identification of UCAs			
Control action	**Not provided**	**Provided**	**Wrong timing or order**	**Too soon or too long**
Change the in-operation line from SGB-NP to SGB-BP through XOV	UCA.1: Control command is not provided when SGB-NP is faulty and XOV is available [SH.1, SH.2,]	UCA.2: Control command is provided when both SGB-NP and XOV are available [SH.1] UCA.3: Control command is provided when both SGB-NP and SGB-BP are faulty [SH.1, SH.2]	UCA.4: Control command is provided too late when SGB-NP is faulty and XOV is available [SH.2, SH.3]	UCA.5: Control command is stopped too soon before XOV is fully closed when SGB-NP is faulty [SH.2, SH.3]

Table 6-6 reports the loss scenarios (SO) using UCA.1 as example. In addition, Table 6-7 identifies the loss scenarios related to the situation that human operator sends the correct control command to change from SGB-NP to SGB-BP but it is not followed or improperly followed by automated controller. The countermeasures for identified loss scenarios have been derived from analyses carried out for the purpose of this work. It is expected that more detailed analysis with improved results would come with an updated analysis when the SGB has reached a more mature design stage.

Table 6-6 Detailed loss scenario related to UCA.1 and example countermeasures

UCA.1: Change the in-operation line from SGB-NP to SGB-BP through XOV is not provided by SCM/SEM on command from human operator when SGB-NP is faulty and XOV is available [SH.1, SH.2]	
Loss scenarios	**Suggested countermeasures**
SO.1 for UCA.1: Human operator receives correct feedback but interprets it incorrectly so SEM/SCM does not receive control command from human operator. The causal factor is that human operator lacks sufficient understanding for abnormal situation.	Must provide the sufficient training for operators to deal with specified hazardous situations.
SO.2 for UCA.1: Human operator receives correct feedback but makes mistakes so SEM/SCM does not receive control command from human operator. The causal factor is that human operator is overstressed when there are too many process to be considered.	The reference document must be presented to provide guidance for operation.
SO.3 for UCA.1: Human operator receives incorrect feedback about conditions of SGB-NP so wrongly believes that the SGB-NP is working but it is not. The casual factor is that the sensor on SGB-NP provides erratic readings.	Sensors must be monitored continuously and be calibrated when erratic reading was detected

Table 6-7 Detailed loss scenario and example countermeasures

Loss scenarios	Suggested countermeasures
SO.4: The control command is initiated by human operator but not received by SCM/SEM. The casual factor is that there is a critical failure on SEM/SCM [SH.1, SH.2].	The status of SCM/SEM must be checked before operation and after each updates.
SO.5: The control command is provided by SCM/SEM on command from human operator, but actuator does not responds to this control command. The casual factor is critical failures on XOV (actuator) [SH.1, SH.2].	XOV must be checked regularly and be repaired when critical failure is revealed.

The suggested countermeasures may degrade or become less efficient considering operating conditions of SGB. For instance, the availability of XOV cannot be guaranteed by continuously monitoring and repair due to maintenance in subsea context may be delayed considering the availability of vessel that transport spare parts. In addition, the cost of some suggested countermeasures may be considerable. For instance, monitoring potential faults in sensor measurements often requires a reference sensor to be installed with additional costs for purchasing and installation. Therefore, designers would like to evaluate the cost-benefit before selecting countermeasures. In this case study, two loss scenarios that caused by erratic reading on sensors are investigated to exemplify:

- Loss scenario 1 (LSO1): Human operator receives incorrect feedback about conditions of SGB-NP due to erratic readings of sensor and wrongly believes that the SGB-NP is faulty but it is not. The control command to stop SGB-NP and activate SGB-BP is provided accidently (SH.1). It is assumed that this situation is recognized after 360 hours and the system operates in reduced production efficiency during this period (L.1).
- Loss scenario 2 (LSO2): Human operator receives incorrect feedback about conditions of SGB-NP due to erratic readings of sensor and wrongly believes that the SGB-NP is working but it is not. The control command to stop SGB-NP and activate SGB-BP is not provided so SGB-NP is not stopped timely (SH.1, SH.2). It is assumed that this situation is recognized almost immediately, but the system must be shut down (L.1, L.2 and L.3) until it can be restored through maintenance.

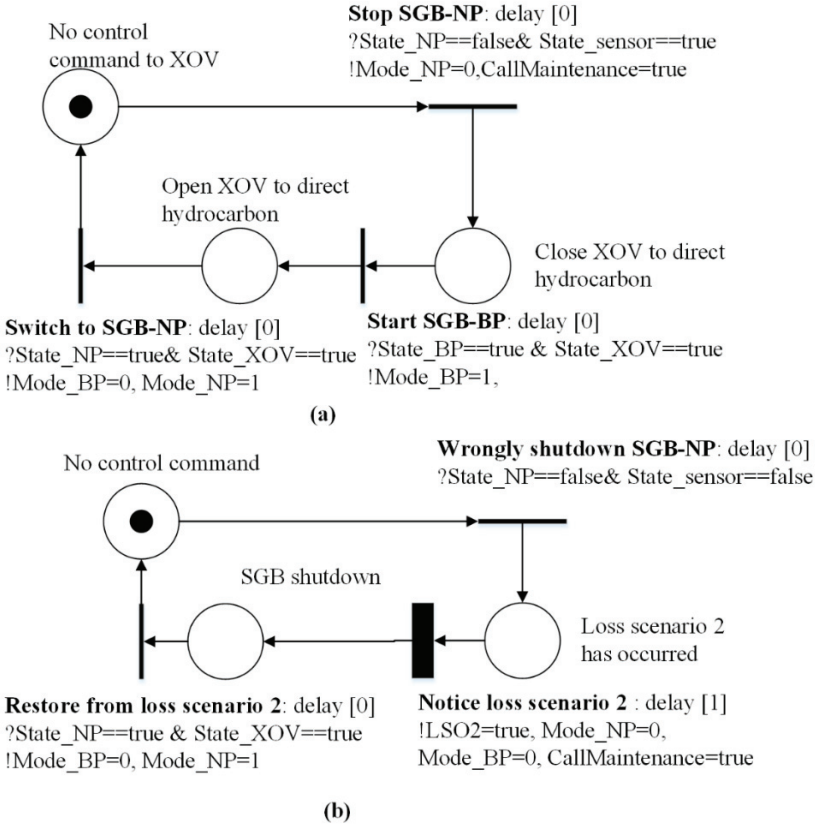


Figure 6-8 Mapping safe scenario and loss scenario into SPN model

Figure 6-8 illustrates SPN for the safe scenario in (a) and loss scenario 2 in (b). The safe scenario is that the control command is provided correctly to switch from SGB-NP to SGB-BP in presence of failure of SGB-NP. Once the failure has been detected, the preparation of maintenance can start (!*CallMaintenance*=true) and SGB-NP is stopped (!*Mode_NP*=0). If both SGB-BP and XOV are available, then the processing line is switched to SGB-BP (!*Mode_BP*=1). After maintenance is completed, hydrocarbon is redirected to normal processing line as the faulty SGB-NP, SGB-BP and XOV is replaced. The loss scenario 2 can occur when sensor provide incorrect feedback (?*State_sensor*==false) in together with failure on SGB-NP (?*State_NP*==false). This loss scenario is immediately detected after 1 hour and the system is shutdown (!*Mode_BP*=0, *Mode_NP*=0, *SO2*=true) and preparation of maintenance start (!*CallMaintenance*=true). After maintenance is completed, the system is restored in the same way as safe scenario. SPN model for loss scenario 1 can be also generated in the similar way. It is assumed that variables related to loss scenarios and safe scenario (State_sensor, State_XOV, State_NP, State_BP) are subjected to system evolution and interventions, which

is described by the RAM model. The variables *Mode_BP* and *Mode_NP* indicate whether there are hydrocarbon flows into the available processing line or not. These two variables are defined in integral domain, whereas the other variables are defined in Boolean domain.

6.4.3 Step II: develop RAM modelling for selected loss scenarios

Figure 6-9 presents SPN model for related variables. The maintenance of hardware component (i.e. SGB-NP, SGB-BP and XOV) is completed together after a certain delay (1440 hours), so the variable *Maintenance* is introduced to synchronize the maintenance events on different piecewise SPN. Since it is assumed that there is no means to reveal the erratic readings on sensor, the sensor is updated through on-line program after 8 hours once both loss scenarios have been recognized (?*LSO1*==true & *LSO2* ==true).

The reliability data for subsea equipment retrieved from the database OREDA [81] are re-evaluated based on discussion with system designer considering the novelty of technology and operating conditions. The estimated data and assumptions for RAM model are as follows:

1) The status of SGB-NP, SGB-BP and XOV is assumed to be under continuously monitoring, thus the failure is immediately revealed. The failure rates for SGB-NP, SGB-BP and XOV are assumed as 3×10^{-5} hour^{-1}, 1×10^{-5} hour^{-1} and 1.5×10^{-6} hour^{-1} respectively. All the failure events are assumed to be exponentially distributed. The sensor is assumed to continuously provide the feedback that is possibly erratic. To compare various control strategies, the four sets of transition rates for this failure mode are assumed as:
    - Case 0: occurrence rate for erratic reading =0
    - Case 1: occurrence rate for erratic reading =0.5×10^{-5} hour^{-1}
    - Case 2: occurrence rate for erratic reading =1×10^{-5} hour^{-1}
    - Case 3: occurrence rate for erratic reading =1.5×10^{-5} hour^{-1}
2) System run with 55% production efficiency when SGB-BP is active.
3) The time for mobilization is 1440 hours. The time of retrieval and reinstallation is delayed for 48 hours. The faulty equipment is replaced (as good as new after maintenance) and the working equipment keeps running as it is (as bad as old after maintenance).
4) The experiment time for simulation is 10 years (i.e. 87600 hours). 5×10^{5} simulation runs have been used for each case. The computation time was

approximately 44 minutes with a 2.60 GHz processor, 16 GB of RAM, and it can increase if there are more variables to observe.

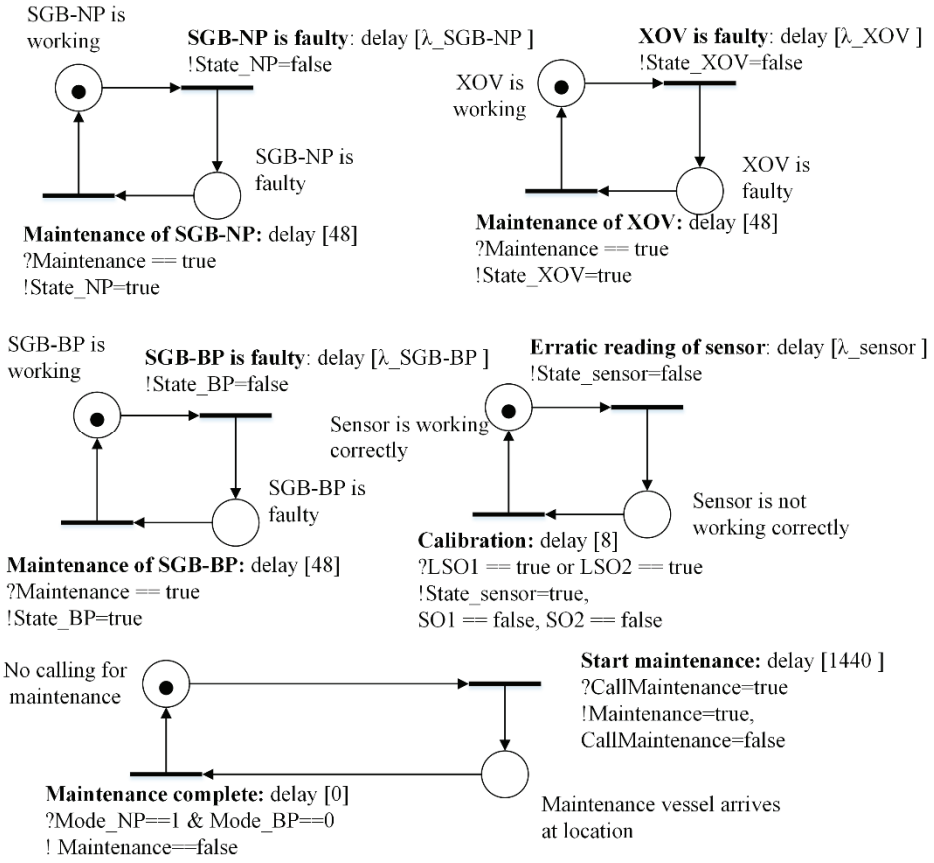


Figure 6-9 SPN model describe maintenance and evolution of controlled process

6.4.4 Numerical results and discussion

The effect of loss scenarios on production loss can be directly calculated through simulation. Figure 6-10 and Figure 6-11 illustrate the average value of system production deficiency and system unavailability from 0 to time t for the case 0-3, respectively. The system production deficiency and unavailability are stated as follow, where the initial value for variable *Mode_NP* is 1, whereas *Mode_BP* is assumed to be 0 as bypass processing line is not working in the beginning of operation.

System production deficiency: 100%-(*Mode_BP*×55%+*Mode_NP*)

System unavailability: 1-(*Mode_BP*+*Mode_NP*)

Table 6-8 reports the frequency of loss scenarios was calculated by observing the frequency of related transitions in SPN. Loss scenario 1 only lead to SH.1, which in worst condition can lead to the production loss (L.1). Loss scenario 2 can lead to all three system-level hazards, which in worst condition can lead to production loss (L.1, L.3) and the hydrocarbon spills accident (L.2). The costs for associated consequence of L.2 given the emergency barrier management can be estimated through ETA if needed.

Table 6-8 Frequency of loss scenario 1 and 2

	Loss scenario 1 (L.1)	**Loss scenario 2 (L.1, L.2, L.3)**
Case 1	7.028×10^{-2} year^{-1}	3.3×10^{-4} year^{-1}
Case 2	1.427×10^{-1} year^{-1}	5.7×10^{-4} year^{-1}
Case 3	2.033×10^{-1} year^{-1}	7.9×10^{-4} year^{-1}

Case 0 shows the situation that the adequate control has been provided for loss scenario 1 and 2, therefore only the safe scenario has been considered. The frequency of loss scenario 1 seems as proportional to the occurrence rate for erratic reading, whilst loss scenario 2 is not. The reason is that loss scenario 1 is subjected to unavailability of sensor (that is proportional to the occurrence rate for erratic reading) and availability of SGB_NP, whereas loss scenario 2 is subjected to unavailability of sensor and unavailability of SGB_NP. The availability of SGB_NP can be seen as proportional to the occurrence rate for erratic reading due to the impact of maintenance in both safe scenario and loss scenario 2, whilst unavailability of SGB_NP is not. The average unavailability and production deficiency in case 0 are 0.0057 and 2.14%, whereas in worst case (case 3) are 0.0148 and 3.08%. If assume that SGB can produce 2 million kroner worth oil and gas per day or 730 million Norwegian kroner (NOK) per year, then the expected difference between case 0 and case 3 is 6.862 million NOK per year in stakeholder's favor.

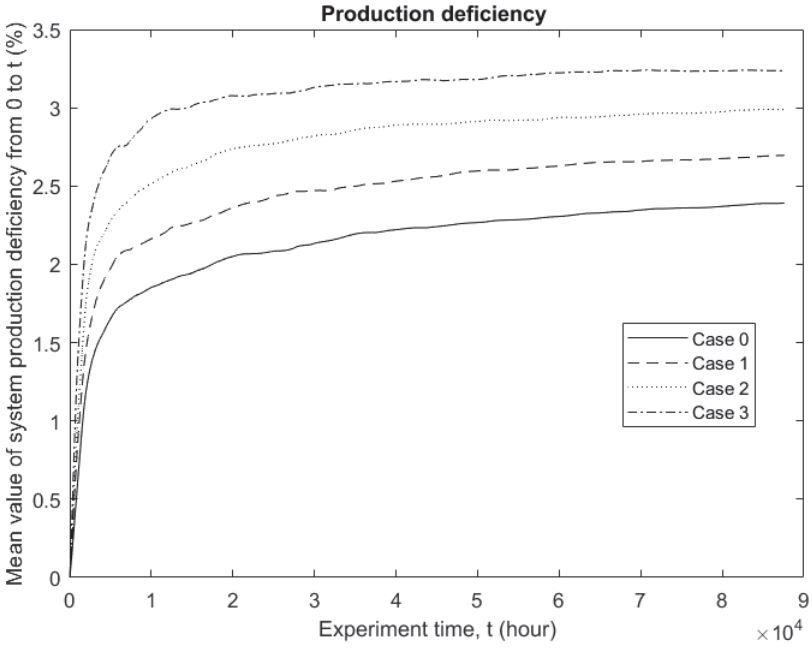


Figure 6-10 System production deficiency of case 0-3

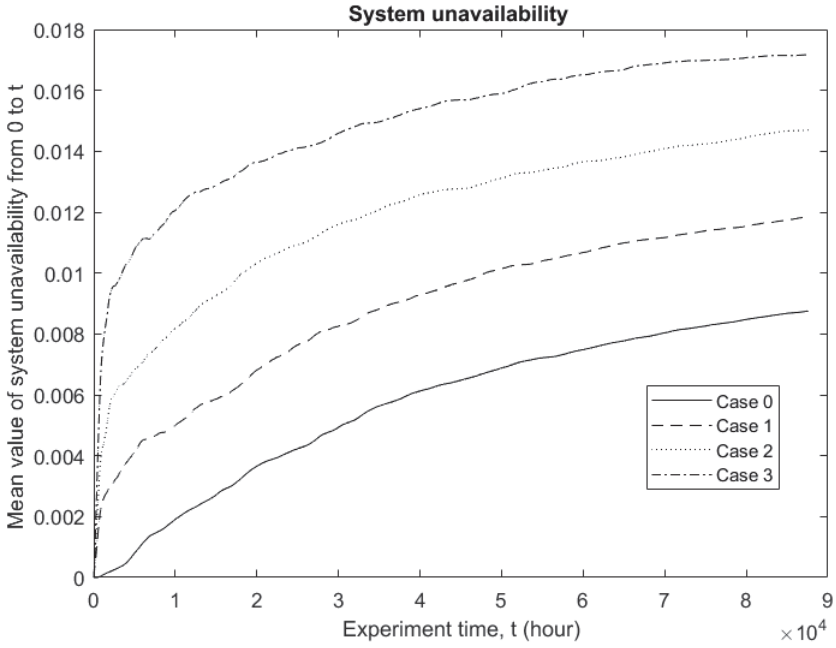


Figure 6-11 System unavailability of case 0-3

It is observed that the effect of loss scenarios is considerable, according to their impact on production and potential for severe accident like hydrocarbon spills. Some example countermeasures are suggested as following:

- Preventive countermeasure is to reduce the transition rate to the state that sensor has the erratic reading. For example, the validity and accuracy of signals from sensors can be increased by removing noise from piping conditions.
- Compensating countermeasure is to increase the ability of controller to discriminate between a real demand and false demand caused by erratic readings provided by sensor. For instance, installation of master sensor that monitors and compares the reading of duty sensor.
- One may also notice that the loss scenario 1 has less severe consequence but higher frequency than loss scenario 2. The system designer may consider to start troubleshooting once loss scenario 1 has been recognized. The premise condition for loss scenario 2 can be removed in this situation since they share the same casual factor and these two loss scenarios cannot occur simultaneously. This said, the hidden error in sensor is revealed and subsequently corrected by a demand.

The selection of compensating and preventive countermeasure depends on frequency of loss scenarios obtained through STPA-RAM modelling and the cost estimation for adverse effects and perceived benefits.

6.5 Discussion

The contribution of STPA-RAM modelling is twofold: (1) to address uncertainty in STPA so its results can be confidently used by decision makers (2) to improve the construction of SPN model taking advantage of control structure offered by STPA.

6.5.1 Level of uncertainty

The proposed approach enables the quantification of hazards derived by a relatively new method STPA, and thereby improve the possibility for decision-making about design choices. It is reasonable to ask to what extent the proposed approach have succeed in this respect. The level of uncertainty is of relevance for making such judgement. In this respect, uncertainty for STPA-RAM model can be categorized into completeness uncertainty that stems from stems from incomplete scope of hazard identification, model uncertainty that stems from low suitability of modelling formalism and data uncertainty that stems from improper

selection of distribution and associated parameter values [70], as illustrated in Figure 6-12.

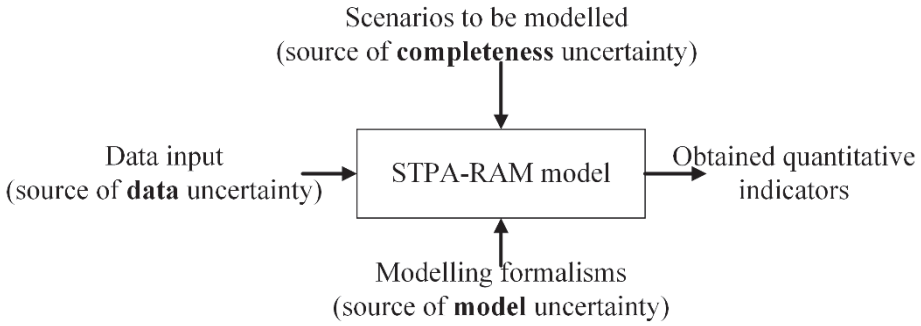


Figure 6-12 Uncertainty related to STPA-RAM modelling

As discussed earlier, human errors and software errors become *visible* in STPA when they are properly defined in the feedback control loop. This feature ensures STPA to develop a (theoretically) complete spectrum of scenarios, where the term *complete* of course depends on the purpose of analysis as done in step 1 of STPA. When the detailed study of STPA is conducted, it is often to get hundreds of UCAs and thousands of loss scenarios. It is practically impossible to include them in one single STPA-RAM modelling due to a significant increase in computational burden. The pre-processing methods for STPA-RAM modelling in this sense are required, for example to eliminate loss scenarios based on existing and planned safety barriers as suggested in [151], or to prioritize loss scenarios based on criticality or risk measures. If the rationales behind these pre-processing methods are specified and documented, the category of completeness uncertainty is reduced.

SPN with predicates and assertions can model loss scenarios without distorting the phenomenon of control structure. The reason is that the use of predicates and assertions using variables can introduce the *validation function* for transitions, which is equivalently the context for safe or unsafe control actions. If Markovian method is implemented instead, the modelling scenarios may be compromised to its mathematical framework (its transitions strictly follow Markov property so it is not allowed to guard the transitions). If the user of STPA-RAM modelling is competent and aware of the limitation of employing SPN, the model uncertainty of STPA-RAM modelling is well acknowledged.

The major bottleneck for STPA-RAM modelling seems to be data uncertainty. The reason is that the loss scenarios derived by STPA move beyond the failure scenarios as the combination of failure modes, whereas most of data resource

collect and record data on basis of failure modes. The probabilistic modelling of loss scenarios is therefore greatly relied on the expert judgement and engineering experience. Rather than abandoning probabilistic model, Berner and Flage [152] elaborated a solution to evaluate the strength of *background knowledge* and beliefs about assumption deviations as supplement to the use of probability tools. The confidence or data uncertainty of STPA-RAM modelling therefore depends on the description of background knowledge that judges and justifies the judgement about assumptions and simplification made. This is remarked as the future work as the potential improvement to the proposed approach.

6.5.2 Pattern-wise SPN model

When dealing with a complex system, it often happens that a large scale SPN model is constructed and remains unreadable and unmanageable [115]. The reason may be the lack of proper description model before constructing SPN model so the construction mainly relies on the imagination of model designer. STPA in this sense can facilitate the model construction of SPN model. The behavior (e.g. failure) of components can be classically modelled by piecewise SPN model.

The remaining question is about how to model the complex maintenance process as control loops, especially for predictive maintenance with the enhanced level of digitalization. Here we propose to model such complex maintenance process as a feedback control loop advocated in STPA: the decision on maintenance is considered as a controller of some sort, the feedback for making decisions are for example the degradation level of component, the control action is therefore to change the state of components for example notifying personnel of maintenance/replacement of equipment. The complex maintenance process is then modelled as a pattern in SPN, for example as shown in Figure 8. The interfaces of maintenance process to other patterns are representing by global variables (e.g. Mode_BP and Mode_NP in Figure 8).

With such a process, the proposed approach can produce the modules of interest (i.e. the patterns) and they can be replicated as many times as need, and make the large-scale SPN model more compact and understandable. By translating description model into SPN model, the causality knowledge can be traceable and updated when hierarchical control structure is updated (for example from step 2 to step 4 in an original STPA procedure). More importantly, when there is more than one hierarchical control structure, the same process can be used to synthesize them and complete in a one single model if necessary. In this regard, it is reasonable to argue that STPA can facilitate constructing SPN model, and

this feature makes STPA-RAM modelling more appealing for systems with complex IMR strategies.

6.5.3 Incorporating software flaws and human errors

As discussed in 6.1.1, software flaws and human errors shall be considered in RAM modelling if they are judged as critical contributors to RAM performance. In the presented case study, software and human-related scenarios (e.g. SO.1 and SO.2 for UCA.1) are not selected due to the lack of reliable probabilistic data. Solving this issue is the task of the next chapter that proposes a procedure for making reasonable estimation on basis of expert judgements and operational experience. If probabilistic data cannot be practically estimated, the checklist of critical loss scenarios should be communicated to stakeholders (e.g. registered as design risks) to evaluate and review the defense measures thus the completeness uncertainty of RAM analysis is not compromised.

If the frequency of software flaws and human errors are determined, they can be incorporated in the same way as hardware failure in STPA-RAM modelling. One interesting issue is that software and human can learn through trials and their errors since they are easier to be altered or manipulated (‘more accessible’, says engineers) than hardware, thus to avoid the same or similar errors when the same context repeatedly occurs [9]. Taking the Figure 6-5 (b) as example, the casual factors considered for loss scenario ‘sending control command too late’ could be the inadequate understanding of unscheduled situations occur. One can assume that the process model of controller can be improved through the lesson learnt. Therefore, the assertion of *Tr5* is ‘$!T=T\times0.5$’ to coarsely model this situation that the delay of detecting abnormal signal is decreased every time this loss scenario happens.

6.5.4 Limitations and constraints

One limitation of the case study is that the loss scenarios selected for the numerical experiment in this paper would normally be identified by traditional failure mode analysis methods. Several authors claim that STPA is able to identify more hazards than traditional failure modes identification method, with regard to software error and interaction type of hazards [142, 144, 145]. For example, one complex loss scenario for SGB design case could be: ‘human operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass processing line, due to a long procedure taken before giving decision or SCU delays in the processing of command to adjust set point of choke valve’. This loss scenario can be prevented by either updating operating procedures (e.g. the procedure must be done within appropriate amount

of time) or modifying the design (e.g. SCU must be able to process the control command immediately).

In case study, only two loss scenarios are modelled. Even some methods for elimination and prioritization of loss scenarios, the number of critical loss scenarios is likely to be more than that. Each loss scenario, or a combination of a few, is regarded as testing experiments of different operational situations. Despite the approach undertaken, it is interesting to investigate strategies for including more loss scenarios in the same model, when this is needed.

In some applications, the evolution of controlled process may be subjected to the shocks from environment, which is not modelled statistically. For instance, if the case study is further refined to study the performance on SPM, then the process variables like 'liquid level on separator' is considered. This process variable is determined by the control command (e.g. open/close liquid discharge valve) and the environmental disturbance (e.g. flow conditions from wells). The change of state of latter one is less predictable than the first one that is subjected to stochastic event. The potential solution for this problem may be to integrate STPA-RAM modelling with the model that studies the physics of controlled process, e.g. finite element analysis. The simulation time is therefore greatly amplified by the agility of process variables, which make the proposed approach unappealing when comes to the industry-scale system.

Chapter 7 Extensions on failure rate predication model

The determination of failure rate is critical to support the qualification of new subsea design. The failure rate of new subsea equipment can be determined by laboratory tests and experiments. Yet, this may not be an option for early design phase where the prototype is not available. It is therefore required to employ the suitable mathematical models to extrapolate failure rate by evaluating RIFs[6] that related to the occurrence of failure, e.g. the application of equipment the exposure from environmental and operating conditions. Many models have been proposed for this purpose, see, e.g. [82, 83].

Two desired extensions are required for these models when they are applied in the early design phase. One is to account for correlation of RIFs, considering many failure modes of subsea equipment share the same or similar set of RIFs due to tight spacing and common-mode connections. Another is to provide possible means to represent the uncertainty when determining the effect of RIFs. Bayesian network is investigated here in order to make these extensions technically possible.

This chapter firstly gives an overview on the previously proposed models for failure rate prediction, and specify why they are reaching limits in the early phase of new subsea design. Then, it proceeds to introduce the basic features of BN, and proposes BN-based failure rate prediction model. Finally, an illustrative example is presented to demonstrate the applicability of proposal, and discuss its usefulness and further improvements.

The main content of this chapter is based on the conference paper presented in ESREL 2016 [153], see the appendices for original content.

7.1 Failure rate prediction

7.2.1 The concept and provision of failure rate

The term *failure rate* can have two meanings: (1) parameter associated with a probability failure density model, (2) the frequency of occurrence of failures, calculated on the basis of the probability failure density. The second interpretation is used here.

The failure rate of an equipment (denoted as λ) and exhibited by a bathtub curve that consists of three phases: (1) *infant mortality* phase where design defects are discovered so the failure rate is expected to decrease rapidly, (2) *useful life* phase

[6] Reliability influencing factors

where the failure rate remains stabilized for a long period, and (3) *wear-out* phase where the equipment exceeds its specified lifetime so the failure rate is increased. If not specified in particular, hereafter the failure rate λ is assumed to be constant (i.e. comes from the useful life phase) and expressed as the multiplicative inverse of mean time to failure (MTTF). It means that the failure occurs according to a homogeneous Poisson process, alternatively, exponentially distributed time to failure. If the defining reliability is the probability of system surviving, it can be expressed as the equation below, where $F(t)$ denotes the cumulative distribution of function and the accumulated time in operation or service is denoted by t [106]:

$$R(t) = P(T > t) = \int_t^{\infty} f(x)dx = 1 - F(t) = 1 - \int_0^t \lambda e^{-\lambda\tau} d\tau = e^{-\lambda\tau}$$

The failure rate of equipment can be obtained from generic database published by an organization that merges data from different places, such as plants, owners, manufacturers and contractors [37]. In O&G industry, the most commonly used database is OREDA [81] that collects and analyzes the data from participating O&G companies, mainly for topside devices and systems. The other databases like exida [154] and PDS data handbook [155] can be used as supplement, and they are mainly for safety systems. The more reliable source of failure rate is from costly laboratory-based tests and experiments [156]. This is impractical for early design where the prototype is not available, thus the data from generic database should be used instead.

Yet, the generic failure rate cannot be directly used for new system that employs new technologies or operates in new environment. Here considers new subsea design as example. The subsea technology is relatively new and lacks of operating experience, and its environmental conditions (e.g. water-depth, pressure and temperature of wells) differ largely from that of existing (topside) systems where the generic data (i.e. OREDA) is collected. This requires efforts to provide useful estimate of failure rate for new system, on basis of generic data or other types of information if the generic database does not exist. Such elaboration is called *failure rate prediction* in this thesis, where the word 'prediction' is to emphasize that it targets new system where experience and knowledge are sparse. The interchangeable terms can be 'reliability prediction' and 'failure rate estimation' that are also commonly used in literature, such as military standard [62].

7.2.2 Models for failure rate prediction

There has been many models for failure rate prediction. The common assumption is that the failure rate of equipment is sensitive to a set of measurable

factors. Hereafter these factors are called as reliability influencing factors, denoted as RIFs. A RIF presents a certain condition that can be monitored or observed, and it is ideally to be constant (e.g. the feature of material) or has small variations associated with time (e.g. temperature and pressure). The RIF can be categorized mainly with respect to the lifecycle and resource perspective (subsection 6.1.1). For lifecycle perspective, they can come from design and manufacturing phase (e.g. material selection), or more likely operational phase (e.g. wear, fatigue, operation loading and stress from environment).

US military standard MIL-HDBK-217F [62] has proposed two models for failure rate prediction of electronic equipment, named *part count* and *part stress*. The part count model is to predict the failure rate by summating all base failure rate at the reference condition. It is simple and requires few information, but is often criticized for giving too pessimistic estimation. The part stress model is to predict the failure rate of an item by studying multiple stress from environment and operation that results in component failure. The part stress may provide a more confident failure rate, but may not be feasible for complex system where mutual correlations between stresses exist [61]. Yet, both two models primarily rely on information collected from laboratory-testing and manufacturers, and the related guideline is no longer updated since 1995 [157]. Then, they are not further discussed.

The proportional hazards (PH) model is used instead [106]. In a PH model, two inputs are required. One is the baseline failure rate (denoted as λ_0) that can be determined at known applications, for example obtained from generic database. Another is a set of covariates (i.e. RIF) assumed to be multiplicatively related to the failure, denoted as $\pi(z)$. Then, the failure rate of equipment in the new application, denoted as λ_{new}, is estimated as follow:

$$\lambda_{new} = \lambda_0 \pi(z)$$

Various models are proposed based on PH model, see a summary in [157]. Two models are selected as representatives here. One model is proposed in barrier and operational risk analysis (BORA) project, where human and organizational related RIFs are considered for the failure event 'hydrocarbon leaks' in O&G activities [158]. Another model is proposed by Brissaud et al. [82], where design-, manufacturing-, installation-, use- and maintenance-related RIFs are considered thus it is more useful for generic systems compared to BORA model. Using these two models normally requires extensive data and information to determine the value of RIFs and their influencing function to the defined failure. Therefore, they are not very practical in early design phase.

Driven by the scarcity of required information for PH-based models, some other models are proposed in particular to account for novelty of technology. Brissaud et al. [159] have proposed a failure rate prediction model for new transmitters, by analyzing relationship matrix of two-levels: structure and functions. Therefore, only the functional and physical specifications are needed. Rahimi and Rausand [83] have proposed a model to extrapolate failure rate of new subsea system based on the data of topside systems, e.g. from OREDA [81]. The main principle is to analyze the relevance between a set of RIFs applied subsea and a set of RIFs applied topside. Both of these two models may be applied for generic system within some minor modifications, even this issue is not particularly elaborated in related articles.

Some extensions may be needed when these models are applied in the early phase of new subsea design, given the following considerations:

1) For PH-based models and Rahimi and Rausand [83] model hold the assumption on the independence between failures, which may not be valid for subsea cases. The tight spacing of equipment, proximate production steps and common-mode connection of new subsea system (see explanation in subsection 3.2.2) imply that different failures may share the same set of RIFs. This implies the need to account for correlations between covariates, especially when they are not reasonably judged as negligible.
2) The crude failure rate obtained in the initial phase may be subjected to a high level uncertainty resourced from parameters used for determining the effect of RIFs. Then, the failure rate prediction model is desired to handle the uncertainty.

Bayesian network (BN) is introduced to account for these two considerations. BN refers to a mechanism of applying Bayes' theorem to model variables and their cause effect relationships. BN is featured by its inclusion of conditional dependencies between variables and its ability to update observations of variables. BN has experienced a growing success in many disciplines such as artificial intelligence development, and it has received growing interests in field of RAM analysis. BN models have been applied for solving various RAM-related topics, such as diagnosis assessment and maintenance planning [160, 161], data uncertainty involved in data collection and statistical evidences [76] and CCF modelling [162]. The next subsection discusses the fusion of BN to failure rate prediction model.

7.2 BN-based failure rate prediction model

A BN model can be expressed graphically. It consists of directed acyclic graph (DAG) formed by variables together with the directed edges, and conditional probability tables (CPT) assigned the conditional dependencies between variables [163]. When a link connects a node A to another node B, A is called as parent to B and the variables that the two nodes denote are conditionally dependent. If the node A has not any parent, it is called as a root node and its prior probability should be specified in the CPT. The posterior probability can therefore be computed by taking advantages of Bayes' theorem [164]:

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B)}$$

In such setting, the posterior probability of nodes A or B can be re-estimated when the adjacent nodes B or A can be changed accordingly, through the statistical dependencies specified in CPT.

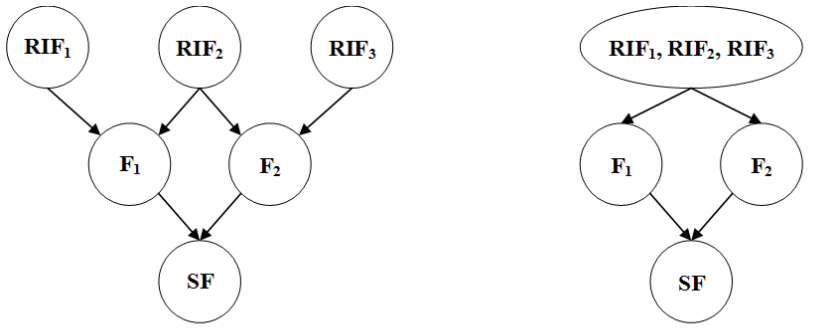


Figure 7-1 BN models of RIFs, component failure and system failure rate

The variables used for failure rate prediction can be easily mapping into a BN model. For illustrative purpose, only three groups of variables/nodes are considered here: *RIF*, *component failure*, and *the failure of system* that consists of various components[7]. As shown in Figure 7-1, RIFs are represented as outermost parent (root) nodes. They are connected to a set of node F_j by causal arcs, meaning they have impact on the selected component failure. Similarly, all component failures contribute to the system failure node, denoted as SF. In the

[7] The users may introduce more cause-effect relationships, for example between RIFs and failure mechanism, if it can be reasonably argued and sufficiently quantified.

Figure 7-1 (a), the root variable RIF_i are assumed uncorrelated, and RIF_2 relates to both failure modes F_1 and F_2. In Figure 7-1 (b), the root node consists of all the correlated RIFs so that the joint probability for all RIF_i should be specified in the CPT, which can avoid incorrect inclusion of dependent RIFs. The joint probability distribution of a set of variables $[X_1, X_2 \ldots X_i]$ is given as follow, where $Pa(X_i)$ refers to the parent node of X_i:

$$\Pr\left[X_1, X_2, \ldots X_n\right] = \prod_{i=1}^{n} \Pr\left[X_i \middle| Pa\left(X_i\right)\right]$$

Then, the first step is to determine the relevant RIFs for component failures. The selected RIFs must be exhaustive enough to explain the potential failure. There are some checklists of generic RIFs, see e.g. [165] and [82]. The user should judge their relevance for the system being studied, for instance to study the physical insights behind the failure in together with experts (e.g. system designers).

The RIF can be defined as a continuous variable or a variable with discrete state. According to the Bayesian philosophy, a random variable A, with some density function of $f(A)$ that can express what one thinks about the occurring value of A, before any evidence are obtained [106]. Therefore, it is possible to account for the effect of uncertainty by allocating suitable probability distribution, for example, the beta distribution for continuous variables [166]. If one variable A in a binomial distribution is beta distributed within prior shape parameter α_0 and β_0, the posterior probability of A is still beta-distributed within posterior shape parameter α_0+s and β_0+n-s, where s denotes the number of n trials that have outcome as outcome X. For calculation convenience, in the illustrative example presented later only the discrete variables are assumed for each RIF.

The second step is to decide the influencing function between RIF_i nodes and the related F_j nodes. This is an extensive procedure and relies on mutual information (e.g. expert judgements, performance indicators and historical events). A mathematical algorithm has already been proposed in Brissaud et al. [82]'s model include mathematical formula and analytical tools. The users may judge their applicability according to the system being studied.

The third step is to determine the cause-effect relations between F_j nodes and the SF node. Similarly, they are assumed to be discrete events. The F_j node can be of binary state (e.g. working and faulty), or multi-state for systems with various performance characteristics (e.g. 100%, 80% and 60% of nominal capacity). It should be noted that even for the safety system that only includes go/no-go performance attributes, the multi-state can be used when degraded mode of

operation is assumed. For instance, a two-of-three voted safety system can have three states expressed as [fully working (3oo3), degraded working (2oo3), faulty (1oo3 or 0oo3)]. The CPT between F_j nodes and the SF node can be determined by studying how a component failure propagates in the given system structure. Here, FTA is used to model failure propagation, thus the top event of FTA is the SF node. As discussed by Bobbio et al. [167], FTA can be mapped into BN model, where each binary event in FTA can be represented by the binary in BN. Therefore, the CPT between F_j nodes and the SF node is established following Boolean logics. In this setting, the effect of RIFs on failure rate can be directly observed in the measure of system reliability (i.e. the posterior probability of the SF node).

Table 7-1 reports three stages for BN-based failure rate prediction. In the early phase of new subsea design, the main focus is to determine initial parameters associated with the RIFs and estimate what is a first estimation of the failure rate of the equipment. Such crude estimation is subjected to a high level of uncertainty. One part is associated with prior beliefs of RIFs. Another part comes from using expert judgements, historical data and operational experience from similar application to determine the influencing functions. Therefore, it is interesting to investigate how to update the estimation, when new evidence is available in the later stages.

Table 7-1 Alternative applications BN-based failure rate prediction

Stages	Main focus
Early design	To include of RIFs and component and obtain an approximate estimation
Detailed design	To renew and update the estimation, with data from accelerated life testing or later from full-scale (site acceptance) testing before operation
Operation phase	To enable forecasting and early detection of changes in trends that may suggest an increase or decrease of reliability.

The term *evidence* here refers to the new information to change probability distributions of nodes. There are two types of evidence for BN-based failure rate prediction model. One type is associated with Fj node, meaning that the occurrence of failure is observed. Such evidences can be collected from accelerated life testing and site-acceptance testing when the prototype is ready. Then, the estimation can be updated by using influencing algorithm within cumulative collection of failures over a certain interval [164]. In this respect, BN-

based failure rate prediction allows the modification of generic input along with prototype development. In addition, the confirmation of influencing function may be needed, given the new estimation of failure rate.

Another type of evidence is associated with RIF_i nodes. Some RIFs can be directly observed based on condition monitoring, or calculated by indirect or inferential information sources (e.g. process parameters) in the operational phase. It allows to re-estimate failure rate/ system reliability given the varying operating conditions. Here consider liquid boosting module on SGB as an example. It is used to ensure the flow from field at the required rate after pressure declines in the reservoir. The failure rate of rotating pump is subjected to the working load (or more specially, the rotating speeds). The operator may adjust the set point of pump speed in case of there is significant change of pressure of hydrocarbon. One potential case is that hydrocarbon flow from the adjacent SGB is redirected into the working pump as the result of reconfiguration (see the explanation in section 6.4). The more likely case is that the pump speed is adjusted according to the change of composition in the flow and the increase of water cut. It is therefore reasonable to argue that BN-based failure rate prediction model can serve as an on-line means to predict failure rate/system reliability in the operational phase. It also calls for special preparations and concerns in the early design phase. First, it must be possible to measure or evaluate the selected RIFs, thus associated requirement for condition-monitoring must be formulated and implemented as early as possible. This can be technically possible through the communication platform offered in RAM-SE framework (see section 5.3). Second, the measurement and evaluation of selected RIFs must allow differentiation in the operational phase.

7.3 An illustrative case: high integrity pressure protection system

This section presents an illustrative example to show the suitability of BN-based failure rate prediction model in the early design phase.

7.3.1 System description

The high integrity pressure protection system (HIPPS) is normally combined with PSD system to protect the downstream equipment from the source of overpressure [29]. It may be also used means to de-rate the design pressure of long pipeline installed subsea, thus saves the cost for material and fabrication (i.e. lighter and thinner pipeline).

As illustrated in Figure 7-2, the realization of HIPPS function is decided on three modules: (1) a module of three PTs to monitor the pressure of equipment; (2) a module contain a logic solver to transmit the operating signals to close the

valve based on 2-out-of-3 (2oo3) voting, meaning that the failure of one PT will not compromise HIPPS function; and (3) a module consists of a HIPPS valve and a pilot valve to stop the flow to downstream facilities under overpressure situation.

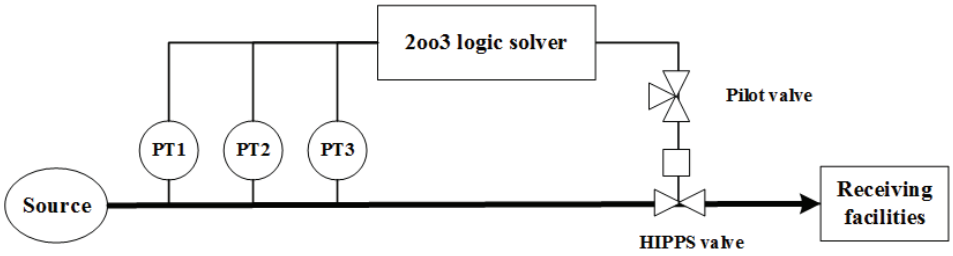


Figure 7-2 The schematic of HIPPS functions

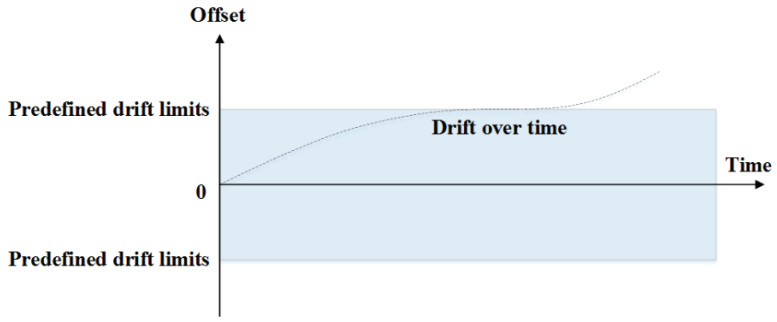


Figure 7-3 Sensor drift over time

The O&G Industry has experienced that the HIPPS function is vulnerable to sensor drift. It is a natural phenomenon (i.e. regardless of vendors) that results in the reading offsets or the erratic reading of pressure sensors, as illustrated in Figure 7-3. If the sensor drift is presented, the information given by the sensor for no longer perfect thus the required HIPPS function is compromised.

In topside (dry) environment, the negative impact of sensor drift could be removed by regular calibrations. When a HIPPS is placed on subsea environment, such calibration requires to retrieve the sensor module, which is not an economically feasible proposition. The new design proposal is to install a new type of sensor that better accounts for the possible drift of sensors. For instance, the sensor can periodically calibrates itself using software implemented compensation combined with other physical measurements (also called as 'virtual/soft sensors', by subsea engineers). The evaluation of new design

proposal for subsea HIPPS requires the *early* indication about the reliability of HIPPS under the effect of sensor drift.

The case study is divided into two parts. The first part is to develop reliability modelling for HIPPS function where the effect of sensor drift is not considered. The generic failure rate data from [81] is used. The second is to extend the obtained model to consider the effect of sensor drift. Since it is an illustrative case rather than an extensive and realistic study, only a limited number of states and nodes is assumed for computation convenience. The trial version of HUGIN [168] is used here for graphical representation and computation of BN-based failure rate prediction model. The mathematical software Matlab with Bayesian network toolbox [169] can be used alternatively when the number of nodes exceeds the limits of trial version of HUGIN.

7.3.2 Reliability model of HIPPS function

The reliability of HIPPS function can be modelled by FTA. As shown in Figure 7-4 (a), each basic event represents the failure of the associated component. The FTA model can be complied into BN model as shown in Figure 7-4 (b). For instance, the basic events that represent 'sensor fails to detect pressure' are translated into PT_1, PT_2 and PT_3 node with binary state. The intermediate event 'sensor module fails to detect overpressure' is to represent the 2oo3 voting of PTs, thus the state of node 'sensor module' in BN model is faulty when more than two of nodes 'PT_i' are in the faulty state. Table 7-2 lists the associated failure rate and prior probability of each components, based on the data provided in PDS data handbook [155]. Since the demand rate of HIPPS is lower than once per year, the average probability of failure on demand (PFD_{avg}) is selected as the measure of reliability as suggested by IEC61508 [170]. The PFD_{avg} can be calculated based on the failure rate λ of each component and the test interval τ (i.e. 1 year = 8760 hours) as:

$$PFD_{avg} = \frac{\lambda \tau}{2}$$

Table 7-2 Failure rate and prior probability of root variables

Root variables	Failure rate (per hour)	Prior probability (PFD_{avg})
PT	0.3×10^{-6}	1.314×10^{-3}
Logic solver	0.1×10^{-6}	0.438×10^{-3}
Pilot valve	0.8×10^{-6}	3.504×10^{-3}
HIPPS valve	2.1×10^{-6}	9.198×10^{-3}

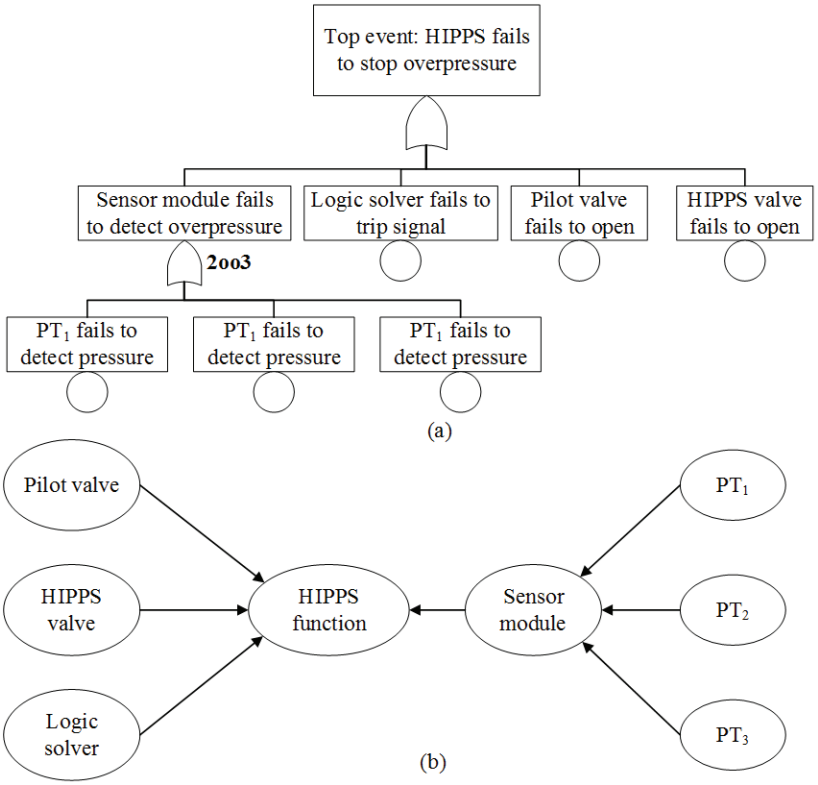


Figure 7-4 (a) FTA model for HIPPS function (b) BN model for HIPPS function

Based on the BN model, the posterior probability of the HIPPS function is calculated as 1.3107×10^{-2}. This result is valid if the degraded mode of sensor module (i.e. one PT is failed) is assumed to have no impact on the execution of the HIPPS function. In addition, one can study criticality of components by selecting most probable explanation (MPE) in BN model. MPE computes the probability of most likely configuration that leads to state where the evidence is given. For instance, if the failure of HIPPS function is observed (i.e. the state of node 'HIPPS function' is forced to be faulty), the most likely explanation is that HIPPS valve is faulty and other equipment can respond on demand, and the probability of MPE is given as 0.004843.

7.3.3 The impact of sensor drift

It is now to extend the existing BN model to consider the effect of sensor drift on the reliability of HIPPS. Various factors can influence the magnitude of sensor

drift, such as material selection, installation, and environmental conditions (e.g. temperature and pressure) [171]. After negotiating with system designers, the operation-related RIFs are foreseen to be important for evaluating the effect of sensor drift. The prior beliefs of RIFs can be approximately decided in the early phase according to historical operational experience, functional specification and the result of operational analysis (of RAM-SE framework).

In this case study, two anonymous RIFs are tacitly assumed for sensor drift, simply denoted as 'RIF_1' and 'RIF_2'. They are connected to their child node 'Drift'. The relevant assumptions are made as follows:

- The state of 'sensor module' is assumed to be conditioned on sensor drift. Sensor drift may be present in all three PTs at the same time, but the degree of drift can be different. It means that the number of functioning sensors can influence the probability of sensor module responding to a high pressure condition. Therefore, the node of 'sensor module' in Figure 7-5 has the ternary state instead of binary state in Figure 7-4 (b), to model the effect of sensor drift when only a single PT is faulty.
- The sensor drift starts after installation, and sensors will experience different levels of drift during each test interval. In this illustrative example, the sensor drift is assumed as discrete distributed in the early evaluation.
- These RIFs are assumed to be disjoint, and they only influence whole sensor module instead of individual PT. If the design-related RIF is selected, for example 'material of sensor', it should be connected to PT_1, PT_2 and PT_3 as it relates to the failure rate of sensor.

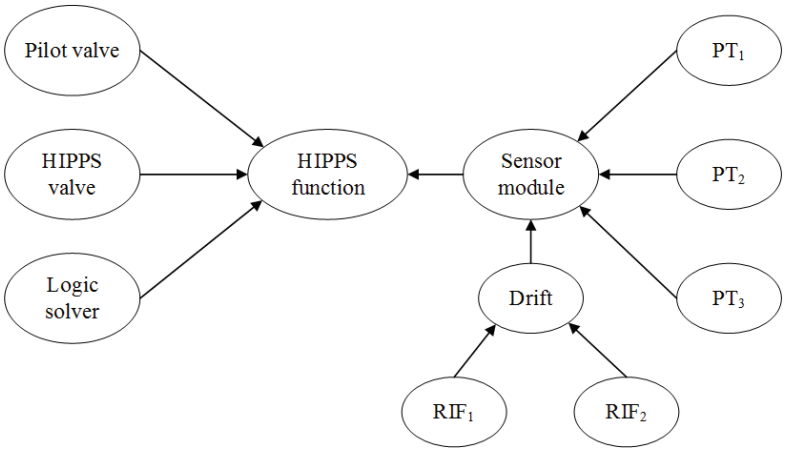


Figure 7-5 BN model that incorporates the effect of sensor drift

Table 7-3 reports the CPT between nodes ‘Drift’ and ‘sensor module’. The node ‘Drift’ is modelled as a discrete node with ternary state: ‘High’, ‘Medium’ and ‘Low’. For instance, when the effect of sensor drift is high and only two PTs can respond, the probability of sensor module is estimated as 0.015. The assigned value is determined on the expert judgments and technical reports. The value of state ‘faulty’ of ‘sensor module’ for all states of ‘drift’ is assigned as 0 then omitted in Table 7-3.

Table 7-3 The CPT between nodes ‘Drift’ and ‘sensor module’

	Drift		
Sensor module	High	Medium	Low
Degraded (2 PTs are working)	0.015	0.01	0.002
Working (3 PTs are working)	0.01	0.005	0.001

Table 7-4 Part of CPT for nodes ‘RIFs’ and ‘drift’

RIF_1	-1 (0.1)		0 (0.9)		+1 (0.1)	
RIF_2	+1 (0.83)	-1 (0.17)	+1 (0.83)	-1 (0.17)	+1 (0.83)	-1 (0.17)
High	0.4	0.1	0.15	0.05	0.1	0
Medium	0.35	0.2	0.05	0.1	0.15	0.01
Low	0.25	0.7	0.8	0.85	0.75	0.99

Table 7-4 reports the estimated conditional probabilities between nodes RIFs and ‘drift’, where the extensive procedure of scoring and weighing of RIFs is not shown in this illustrative example. The outcomes/states of RIF1 are assumed as trinary, i.e. -1, 0, +1, meaning that RIF1 has negative effect, no effect, positive effect on the magnitude of sensor drift. The outcomes/states of RIF2 are assumed as binary, i.e. -1, +1, meaning that RIF2 has negative effect and positive effect on the magnitude of sensor drift. The prior probabilities of RIF1 and RIF2 are given as [-1(0.1), 0(0.9), +1(0.1)] and [+1(0.83), -1(0.17)], expressing what one (e.g. the expert) thinks about the probabilities of states of RIFs. For instance, the distribution of sensor drift effect is estimated as [0.4 (High), 0.35 (Medium), 0.25 (Low)] under the situation that RIF1 has negative effect (i.e. the outcome of RIF1 is -1) and RIF2 has positive effect (i.e. the outcome of RIF2 is +1).

The posterior probability of the HIPPS function is now slightly increasing from 1.3107×10^{-2} to 1.5345×10^{-2}, considering the effect sensor drift. The result of MPE indicates that the HIPPS-valve is the most likely one to be blamed if failing to perform HIPPS function in case of over-pressurization. Therefore, one may conclude that: when the subsea HIPPS is influenced by sensor drift that is estimated in this example, the most vulnerable component is still the HIPPS valve until sensor drift reaches the pre-defined acceptable limit.

The state of RIFs be continuously updated if the new information is available, e.g. the (early) simulation result. For instance, if the failure of HIPPS function is observed during operation, the posterior probabilities of RIF_1 and RIF_2 can updated as [-1(0.08), 0(0.82), +1(0.1)] and [+1(0.42), -1(0.58)] respectively.

7.4 Discussion

As shown in the illustrative case, the model provides an 'approximate but more closed to reality' failure rate, which reflects the best knowledge available in early design phase to decide to what extent they can be foreseen as important. Rather than discussing the implication of estimation itself, it is more meaningful to discuss how it is obtained from the suggested heuristic model.

In this chapter, BN is demonstrated to extend the application of existing failure rate prediction models (e.g. [83]). BN can account for conditional relations between RIFs and failure modes, which is assumed for subsea system, and has ability to incorporate uncertainty, which is required by early design phase. In addition, BN-based failure rate prediction model is theoretically feasible as design proceeds, and even useful in operational phase. The model developed in the early design can be further extended by adding the casual arcs or variables, and the estimation can be continuously renewed through the evidence collection from the different phases of system development.

Yet, the BN-based failure rate prediction model is subjected to the following limitations:

- The detailed procedure to assign the prior beliefs of RIFs is not described in this chapter. This is especially important and challenging for design-related RIFs, such as materials selection. The practical solution is to carry out a survey among manufacturers, suppliers and experienced operators to decide the magnitude of RIFs.
- The detailed procedure to determine the influencing functions is not described in this chapter. In the proposal, the algorithm proposed by Brissaud et al. [82] is used as alternative. However, it has difficulties

to find reliable expert judgments. The possible direction is to rely on the experiences from similar equipment. For instance, the RIF of sensor drift can be 'the pressure inside pipeline'. The subsea sensor's interaction with the flow being measured can be similar to that in topside plants. The experience and data of topside technology (that is more readily available) can be useful in determining the influencing functions of RIFs on subsea systems, with reasonable judgments about its application-relevance.

The identification of RIFs relies on the means to ensure the proper communication between RAM analysts and system designers. For instance, the monitoring and measurement of operation-related RIFs may demand modifications to current design concept. If the selected RIFs are not exhaustively to explain the failure mechanism, it should be documented and registered as the design risks.

Moreover, BN-failure rate prediction model can be used for estimate the frequency of software flaws and human errors, which is the remaining problem in the previous case study (see discussion in section 6.5.3). The BN-based failure rate prediction model can be also used to reasonably assign the probabilistic data for software flaws and human errors. The major challenge may be to determine a manageable set of RIFs of relevance to human errors and software flaws. The BORA project [158] has given a list of generic human and organizational factors that relate to hydrocarbon spills in O&G activities, which may be considered as an reliable reference. The most disturbing part seems for software-related RIFs, where the software does not follow the physical laws of degradation and failures as for hardware. Moranda [172] have proposed detailed mathematical models for failure rate prediction of software, and their extensions with BN are underlined as future work.

Chapter 8 Guideline of RAM modelling

RAM modelling is to calculate the probabilistic indicators about RAM performance for a given system concept. Many formalisms are currently used in RAM community. RAM analysts should be aware of their modelling power and limitations, otherwise model uncertainty may arise from low suitability of chosen model. Resolving this issue requires the sufficient knowledge in selecting and constructing RAM modelling formalisms.

The guideline developed by ISO/TR 12489 [9] can be a good starting point. The extensions are needed, however, given the constraints posed in early phase of subsea design. First, the existing guideline is mainly used for safety systems and few attention is paid to the modelling of multi-state and multi-unit, which is generally assumed for subsea production and processing system. Second, the selecting criteria suggested by ISO/TR 12489 [9] involves some degrees of subjective. For instance, it suggests to distinguish the 'strong dependencies' and 'weak dependencies', which is subjected to large degree of interpretation in a subsea context.

This chapter aims to propose the modification as necessary complementary to existing practice in selecting and developing RAM modelling for new subsea design. The point of departure is to compare the commonly-used modelling formalisms. Then, it proceeds to formulate the general modelling issues for subsea production and processing system. Finally, a new guideline on selecting formalism to construct RAM modelling is presented, and its advantages and feasibilities are discussed.

8.1 Commonly-used modelling approaches

Figure 8-1 presents the scope of commonly-used RAM modelling discussed in this chapter. They can be classified due to different criteria such as user friendliness, the conservativeness of results and the study objectives [9]. Two high-level and generic criteria are used: *means of calculation* and *nature of modelling*.

Considering the means of calculation, they are based on either *analytical* or *simulation*. The analytical formula can be obtained by Boolean model and Markovian model that are discussed later. The part 6 of IEC61508 [170] provides a straightforward guideline on using analytical formula, where the important contributing factors such as test intervals and repair time are recognized. The potential pitfall is that one may use analytical formulas without awareness to their strict (and often conservative) assumptions as they are published in the

recognized standards [173]. The analytical formula is fairly tractable only for a simple system (e.g. single unit with binary state). The research efforts have been paid to extend the restricted application of analytical formula, see, e.g. [174] regards partial tests and [175, 176] regards K out of N (KooN) configuration. These advanced analytical models result in complicated formulas that are different to comprehend even by skilled RAM analysts.

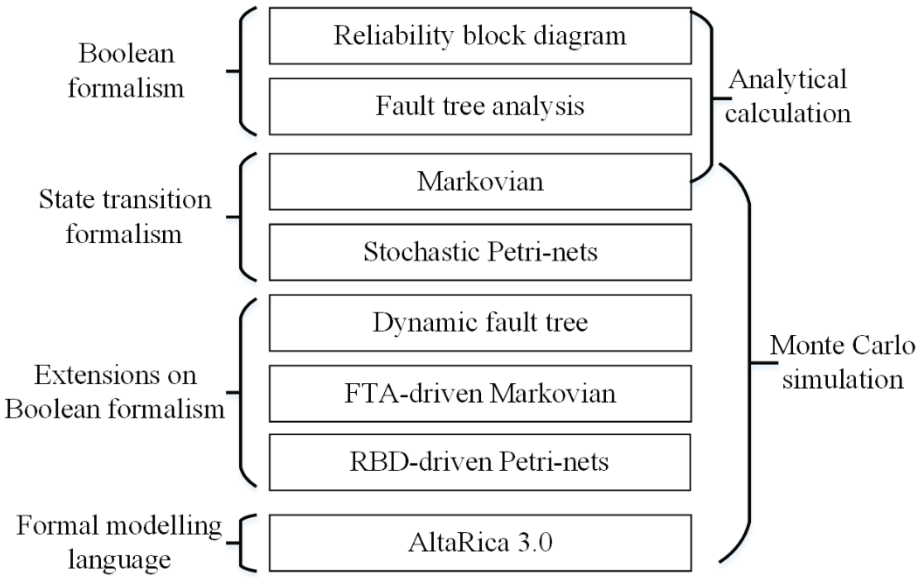


Figure 8-1 An overview on commonly-used formalisms for RAM modelling

In this respect, Monte Carlo (MC) simulation appears to be the feasible option for capture the realistic aspects of complex systems (e.g. multi-unit and multi-state system)[8]. The simulation-based RAM modelling heavily relies on good algorithm and sound mathematical framework provided by the software tools. If RAM analysts lack the basic understanding of mathematics and modelling languages behind the selected software tool, the confidence of RAM modelling can be discounted [9]This thesis will not further discuss the possible errors caused by 'black box' approach used in computational software like GRIF [117] and HUGIN [168], but readers should be aware of this reality.

Considering the nature of modelling, the commonly-used modelling formalisms are classified into four groups: *Boolean formalism*, *state transition*

[8] It has to note that this thesis does not claim that simulation-based modelling is better than analytical formula or vice versa. Indeed, they are used complementary, to verify the produced results from each other.

formalism, *extensions on Boolean formalism* and *formal modelling language*. Two important features are considered to attribute 'the nature of modelling': *flow propagation* and *synchronization of events*. The flow propagation is the feature to describe how the information (e.g. faulty state of component) propagates along the system structure. The synchronization of event is the feature to describe the interplays between failure events and other events (e.g. test and maintenance). These two features determine the *expressiveness* of RAM modelling formalism, which refers to the things represented or being representable. Generally, the more expressive a modelling formalism is, the lower simplicity it has (e.g. less concise and readable to be understood and more computational resource it consumes). In early phase of new subsea design, some expressiveness may be traded for more efficient communication with stakeholders.

The following subsections discuss and simply exemplify these four formalism, in light of their expressiveness and simplicity.

8.1.1 Boolean formalism

The mostly-used models for Boolean formalism are FTA [177] and RBD [178]. The expressiveness and mastery required for FTA and RBD have no significant difference and these two models can be easily converted into each other. The selection is therefore a matter of taste. For example, RBD may be selected given the preference of series-parallel structure, otherwise FTA with tree structure seems more feasible. In the rest of this subsection, FTA is used as example to exemplify Boolean formalism.

As a tree structure, a FTA is made of a *root* and a number of *leaves* that connected by gates. The root is called as 'top event' to represent the failure of system or other types of system-level loss, whereas the leaf is called as 'basic event' to represent component failure or other types of deviations. Following Boolean formalism means that the state of event is binary. The gate is the logic operator to aggregate binary states. The gates of standard FTA includes AND-gate, OR-gate and KooN gate. FTA is commonly used for safety systems, where success/failure of system performance is relatively easy to define within yes/no decision boundary. A multi-state system, for example a subsea production system where the degraded mode of operation is acceptable, is therefore not (at least not in an easy way) properly modelled in standard FTA.

The major advantage of standard FTA (or Boolean models in general) is that the explicit representation of hierarchical structure. This facilitates to represent failure propagation graphically: a component failure combines with other component failures and finally results in a system failure.

The intrinsic constraint for standard FTA is the strict assumption on independences between basic events, meaning that the occurrence of a basic event has no impact on the occurrence of other basic events. FTA may provide adequate approximation when there is weak dependence. The example for weak dependence could be that two periodically tested components share one single repair team (i.e. an remote component interacts with these two components) where repair time is negligible, meaning that the availability of repair team cannot make strong impact on the availability of these two components [9]. Conversely, the accuracy of FTA is unacceptable in case of strong dependences between basic events, such as standby problem. This suggests that Boolean models are only suitable for *static* systems, where independency/weak dependencies between events are reasonably assumed.

The analysis of FTA entails can be qualitative and quantitative. For qualitative analysis, FTA can be used to represent combinatorial characteristics of failure scenario (i.e. a set of basic events), and the failure scenario with smallest size can be determined by minimal cut set theory, see the detailed description in [106]. For quantitative analysis, it can be used to calculate probability of the defined top events.

8.1.2 States transition formalism:

States transition formalism means that the system is modelled as a finite number of *states*, and events enables the *transition* from one state to another. Compared to Boolean formalism, state transition formalism can capture the dynamic features of a system by paying the price of calculability. Markovian model [179, 180] and SPN model [115, 116, 181] are two examples following state transition formalism:

- **Markovian model:**

Markov chain describe a stochastic process where the transition follows Markov (or *memoryless*) property, meaning the future state of a stochastic process only depends on the present state and has no relevance with the sequence of events reaching the present state[9]. This is valid only when the delays associated with each events are exponentially distributed. In reality, some events like repair and periodic test are deterministic events rather than random events. The Markov chain model can give an adequate approximation for modelling deterministic events, when (1) the repair rate restoration (equals to reciprocals of repair time)

[9] It can be mathematically described as that: the state at time $t+\Delta t$ only depends on state at time t, not on time t and state before time t. The constant rate is assumed for each transition.

is much greater than those of failures, and (2) the down time are much smaller than interesting time span.

These assumptions are not valid for periodically tested component where the test interval τ is no longer negligible compared to the time span. Multi-phase Markov chain is proposed to deal with this issue, where the occurrence of deterministic event is modelled as the discontinuity at the given time. As the name suggested, a stochastic process divided into distinct phases and the transition between each phase is delayed by defined time period (e.g. test interval τ) [182]. The specific scenarios for periodic test such as imperfect test and test-induced failure can be reasonably included multi-phase Markov chain.

- **SPN model:**

The detailed introduction to graphical notations of SPN can be found in 6.3.2, thus it is not repeated in this section.

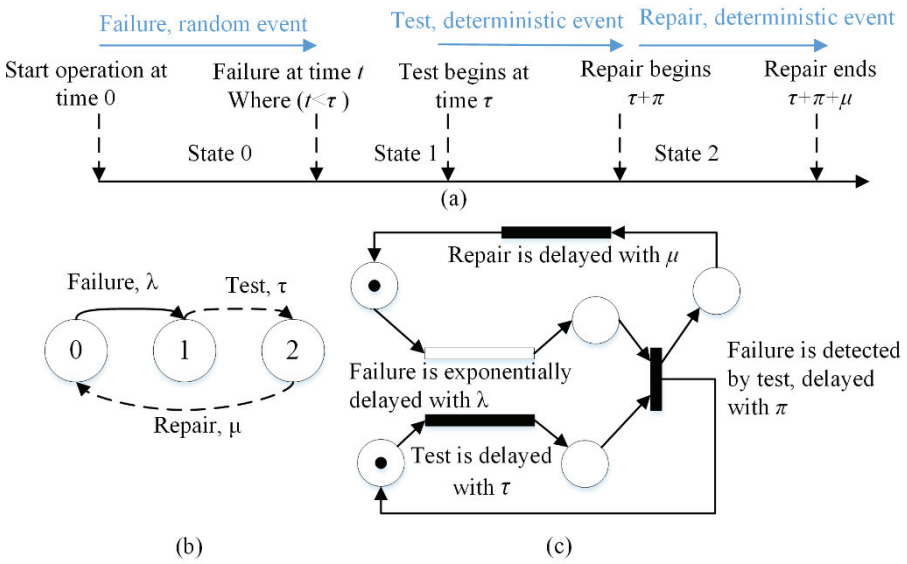


Figure 8-2 Example in (a) a chain of event, (b) Markovian model (c) SPN model

A simple example is used to discuss the difference and similarities between Markovian model and SPN model. There is a single component that is passive and subjected to a constant failure rate during operation. The regular test is performed periodically, and the repair action is followed if component is detected as faulty. This example is as illustrated in Figure 8-2 (a) as a chain of event. A multiphase Markov model is employed in Figure 8-2 (b), where the deterministic

event '*test*' is delayed with τ, meaning that state 1 is forced to be state 2 every τ hours (i.e. test interval). Similarly, state 2 is forced to become state 0 every $\tau+\pi+\mu$ hours (i.e. test interval plus time for test and repair). Figure 8-2 (c) represents the SPN model for the example.

These two models are naturally different in the representation of states. As shown in Figure 8-2 (b), the Markovian model represents the states explicitly, meaning that every possible states must be defined and attached with transitions, thus its size exponentially increases with regard to the number of components. The application of Markovian model is limited to study the degradation process of single component or availability for a system within a small number of components. Brameret et al. [183] have proposed the approach to eliminate trivial states to generate partial Markovian model with acceptable. The SPN model has the implicit representation of states (i.e. the distribution of tokens) as shown in Figure 8-2 (c), thus the size of SPN model is linearly increased. It is reasonable to argue that the state transition model is in principle more expressive than the Boolean model, but this advantage is lost in case of industrial size system (i.e. a considerable amount of components with complex interactions).

In addition, Markovian model and SPN model are different in expressiveness. Markovian model is not compositional [63]. For subsea system the effect of failure is not isolated to one component alone but may embrace many others as well. If the repair of the component in Figure 8-2 is conditioned on other states (e.g. the failure of components in the same module), Markovian model is no longer suitable. The same issue can be managed in favor of SPN model. As shown in Figure 8-2 (c), the scenarios 'component fails' and 'carry out periodic test' are modelled in separate perspectives (i.e. they are with individual tokens). They are synchronized with the fused transition '*failure is detected by the test*', and this transition is valid only when tokens reach the places '*component failure is not detected*' and '*test begins*'. After a certain delay (i.e. the duration of test π), the token reaches the downstream place that represents the state 'detected failure waits to be repaired', which is equivalent with state 2 in Figure 8-2 (b). The other modelling issues like CCF and shared resources (e.g. repair team and power system) by the means of synchronizations. Yet, such representation of SPN model is often unreadable. It is quite difficult (and sometimes error prone) to design SPN model for industry scale systems.

The common limitation for Markovian model and SPN model is that the system structure is hidden. In this respect, state transition model is more 'abstract' (i.e. less readable) than Boolean models. In addition, the lack of system structure makes flow propagation difficult, especially when there is more than one information to aggregate and process (e.g. the degradation of component and the

productivity of system). This is the inherent weakness for Markovian model, whereas it can be relieved in SPN model when predicates and assertions are introduced. The new variables are defined to represent the information flow that can be updated by assertions and synchronized to transition by predicates, see the example provided in 6.3.2.

8.1.3 Extension on Boolean formalisms

Boolean model seems a natural way of modelling multi-unit system due to their ability on representing the system structure. The extensions have been proposed to add dynamic attributes to increase the expressiveness. The representatives are dynamic FTA [184], Fault tree-driven Markovian model [9] and RBD-driven Petri-nets [115].

- **Dynamic FTA:**

The Dynamic FTA extends the standard FTA that encodes Boolean functions, by introducing new logic operators (i.e. gates): priority AND-gate, sequence gate, standby or spare gate and functional dependency gate [185]. The inclusion of these dynamic gates eliminates the strict assumptions on independence between basic events. The practical scenarios like the activation of standby, the failure of cold (i.e. dormant) and hot standby, cascading failures and the example in Figure 8-2 can be well-established in favour of dynamic FTA.

Dynamic FTA has similar expressiveness to state transition formalism and it also requires the simulation tool for computation. Yet, dynamic FTA is less resource-consuming in simulation (i.e. less computational time and less memory for storing the states) [63]. It is reasonable to use dynamic FTA for system with a large number of states.

- **Fault tree-driven Markovian model and RBD-driven Petri-nets**

These two modelling approaches are often named as *Boolean logic driven state transition models*, as they are the marriage of Boolean formalism and states transition formalism to combine their individual advantages. For fault tree-driven Markov model, the basic events are now attached with Markov property and the operation of gates depends on other gates. This allows to model the large scale system and incorporate weak dependencies, such as cold standby systems. RBD-driven Petri-nets model is to decompose the large scale SPN model into blocks following ‘LEGO-principle’, where information flow along with blocks is naturally represented by synchronization of transitions. It has to note that the fusion with Boolean models does make state transition model easier to construct and comprehend, but there is no any significant advance in expressiveness.

8.1.4 Formal modelling language

Foremost, it is needed to define the term *formal modelling language*. The model language is formal when its semantics are defined and a set of rules are specified to them, so the interpretation and execution of model is *formal* (i.e. without any ambiguous) [186]. From this point of view, UML and SysML used in SE domain (they are mentioned in Chapter 5 and some examples are given) are not considered as formal modelling language. Instead, they are considered as a set of graphical notations [63].

One example of formal language used for RAM modelling is AltaRica 3.0. Its ancestor (AltaRica Data Flow) is briefly mentioned in IEC 61508 [39] and ISO/TR 12489 [9]. AltaRica 3.0 combines Guarded Transition Systems (GTS) [187] that generalizes the state transition formalism and System Structure Modelling Language (S2ML) [188] that defines system structuring mechanism stemmed from object-oriented programming. A GTS is a six-tuple <V, E, T, ι, H, B> where:

1. V includes two disjoint sets of variables: the state variables S and flow variables F.
2. E is a set of potential events in a given system structure. The time elapsed for events are called delay, which can be deterministic or stochastic.
3. T is a set of transitions denoted as <G, e, P>. e is an event belong to E. G is the guard (pre-condition) of the transition and P is post-condition of the transition to update the value of predefined state variable S.
4. ι is the initial value of variables.
5. H and B are respectively the head and the body parts of the assertion to calculate flow variables. The assertion in GTS is fix-point calculation, which makes AltaRica 3.0 possible to solve the looped system that cannot be solved in previous version (AltaRica Data Flow).

Figure 8-3 presents AltaRica 3.0 codes to reproduce the example in Figure 8-2. The assumption is that failure rate λ equals to 1×10^{-6}, test interval τ equals to 8760 hours (i.e. one year), repair time μ is 8 hours and test duration π is 2 hours. As shown in Figure 8-3, the system is decomposed into two patterns (i.e. *class*), namely *test* and *component.* The behavior of each pattern is declared by *event*. The *transition* defines all possible switch between states defined in *domain*, and the attributes *init* specify the initial state. The transition is valid when the guard is fulfilled. For instance, the repair of component start when component is faulty (state==FAILED) and failed is detected (detected==true). The delay of transition can be stochastic and deterministic, and its value is attributed by *parameter*. The transition is valid when the guard condition is fulfilled. After firing the transition, the post-condition is updated, for example component is repaired

(state==WORKING). Then, the system structure is declared by the *block* that composes two instances of *class*, and the transfer of information propagation is realized by *assertion*.

```
domain ComponentState = { WORKING, FAILED}          States
class Test
        Boolean test (reset = false);
        event startTest (delay=Dirac(tau)),
        event endTest (delay=Dirac(pi));            Events within
        parameter Real tau = 8760;                  stochastic descriptions
        parameter Real pi = 2;
  transition
     startTest : test-> test := true ;              Transition of states
     endTest: not test- -> test := false ;          based on events
end
class Component
  ComponentState state (init = WORKING);
  Boolean detected (reset = false);
  event failure (delay=exponential (lambda)),
  event repair(delay=Dirac(mu));
  parameter Real lambda = 1.0e-6;
  parameter Real mu = 8;
  transition
     failure : state==WORKING-> state:= FAILED;
     repair: state== FAILED and detected == true-> state:= WORKING;
end
block System
   Component A;                                     System
   Test T;                                          structure
   assertion
   A.detected := T. test
end
```

Figure 8-3 AltaRica 3.0 codes for example in Figure 8-2

From this example, it is reasonable to argue that AltaRica 3.0 has similar mathematical properties as SPN as both of them rely on state automata. The SPN models for case studies of Chapter 5 and Chapter 6 can be encoded by AltaRica 3.0. As object-oriented language, AltaRica 3.0 favors the reuse of classes to make the large-scale model compact and understandable[10]. In addition, GTS introduces the fix point mechanism to update and stabilize the flow propagation [187]. This feature makes AltaRica 3.0 possible to handle network systems (e.g. metro

[10] This feature is unfortunately not explicitly exhibited in the two case studies where the relatively simple systems are selected.

transportation) and looped systems (e.g. power grids) that are unmanageable by SPN model. AltaRica 3.0 can be compiled into other approaches like FTA and Markovian model at no computational costs [189].

There may be some limits for using AltaRica 3.0. First, the use of AltaRica 3.0 is reserved to the specialist with a mastery understanding of state automata and strong programming skills. Second, AltaRica 3.0 may not intended to be used as a universal language, meaning that it cannot solely fulfill every purpose of RAM modelling. There are other modelling language based on state automata, such as performance evaluation process algebra (PEPA)-net and safety analysis modelling language (SAML). The comparisons between AltaRica 3.0 and PEPA-net and SAML can be found in [190] and [191], respectively.

8.2 RAM modelling in early phase of subsea design

Figure 2 of ISO/TR 12489 [9] has suggested a guideline to choose adequate modelling formalisms regarding safety system in O&G industry. For instance, it suggests to distinguish the degree of dependencies (i.e. weak and strong) considering the effect of periodic tests and scheduled maintenance. The 'weak' dependencies are assumed for Boolean formalism and 'strong' dependencies are assumed for state transition formalism. The selection criteria itself is well-argued and does not present any significant disadvantage under the context of safety system. This selection criteria is yet ambiguous and vague in case of a subsea production and processing system, where the other types of events (e.g. delayed maintenance, group maintenance and degraded mode of production) may be assumed. The justifications of original selection criteria may be needed to support selecting modelling formalism, considering characteristics of a system under studied.

It is therefore of utmost importance to define system characteristics at first. In early design phase, the new subsea design is only a concept characterized the high-level functional specification (and possibly the preliminary specification of system structure). This naturally raises the question: *what are the essential information input to properly define the system characteristics and undertake the implementation of RAM modelling*?

8.2.1 From system specification to RAM modelling

In practice, there is always a gap between the written system specification and its realization into RAM model. It means that the development of RAM modelling is subjected to the epistemological entity in the head of analyst, such as worldview and the preference of modelling approaches. If a minor change is made to design concept, the associated RAM modelling has to be revisited, and

the reconstruction of RAM modelling may be required as a domino effect. Such gap also decreases the possibility to update the model by other analysts.

The communication platform in RAM-SE framework is to continuously close the gap by updating the system concept during system development process. The description of system concept can be classified into following three categories, given the increased level of details it possesses:

- **Functional specification**:

This refers to the specification of functions that are of highest interest to secure the defined requirement under normal conditions. In early design phase, it is developed on basis of operational analysis (e.g. use cases) and in form of state-based model (e.g. state diagram) or flow-based model (e.g. activity diagram).

- **Dysfunctional analysis**

This is based on functional specification to study system performance in presence of foreseeable abnormal events. The example models have been discussed in subsection 6.1.2, such as FMECA and HAZOP. These traditional models are easy to build up and convenient in communication with engineers and contractors, but they have limitation in explicitly expressing the dependencies between events. Therefore, they are often suffer to be far from RAM modelling. One exception is STPA. The section 6.3 has proven that STPA can be easily converted into SPN model without too much effort, taking advantage of finite state automata. In addition, employing control structure offered in STPA facilitates the construction of pattern-wise SPN model (see discussions in 6.5.2).

- **Modelling issues identification:**

This aims to fill the gap between system specifications and RAM modelling. This task should be naturally embedded when constructing RAM modelling, however, sometimes omitted and lack a structured approach. There are four main aspects covered in modelling issues identification:

- **System structure**: it is to describe the relationship between each element including hardware, software and organizational factors. The typical relationships are hierarchical (adapted in FTA) and distributed. In a distributed system, elements share the resource and capacity to fulfill the single objective (e.g. production). In other words, distributed system is more complex since its behavior is attached with strong dependencies. Different models built up on particular interests of the same system can be related one another through the system structure.

In RAM-SE framework, (functional and physical) decomposition is recommended for modelling hierarchical system structure, and DSM is recommended for modelling distributed system structure.

- **State:** it is a set of possible conditions that a given element could be. For safety systems where only functional and dysfunctional properties are considered, the state of element is assumed to be binary. For production systems normally with variable performance characteristics, multi-state is assumed for given elements. In RAM-SE framework, state diagram is used for obtaining the full spectrum of state.
- **Event:** it is a set of triggers for transitions between states. For RAM modelling, the spectrum of events can be given as a set of triplets, <*F*, *T*, *R*>. *F* denotes the failure event, which is assumed to be a stochastic process. *T* denotes the event to confirm the state in response to *F*, which can be continuous monitoring or periodic test. *R* denotes the event that brings the system from the abnormal state back to the normal (e.g. repair and maintenance) or other functioning state (e.g. switch to standby or degraded mode). Ideally, *R* and *T* are considered as deterministic. The event-centric description is naturally embedded in FFBD or activity diagram that are recommended in RAM-SE framework.
- **Reliability data**: it refers to the stochastic description for each set of < *F*, *T*, *R* >. The failure event is subjected to the natural randomness of system, which may not be easily revealed in the early phase of new design. Chapter 7 has discussed the practical model for solving the scarcity of data for failure events. The reliability data for test and repair event are more accessible even for new design, as they are largely dependent on operator's decisions.

Every formalism for RAM modelling includes these four aspects for the system under study, but the representation of these aspects varies according to the formalism in use. For instance, FTA seems more suitable for hierarchical system structure within binary states. SPN and AltaRica 3.0 are feasible to model multi-state system within strong dependencies between events.

8.2.2 Modelling scenarios of subsea system

The modelling scenarios can be identified by studying the logic structure of triplet <*F*, *T*, *R*>. The expressiveness of RAM modelling depends on the degree that the modelling scenarios in compliance with the selected formalism. The

following presents assumptions for possible modelling scenarios of new subsea design.

- **Advanced property of deterministic events, *T, R***

This mainly refers to side-effects of test and maintenance activities. For safety systems, a proof test is designed as realistic as the real demand to give more credits on the confirmation of robustness, which lead to the fact that the stress introduced by a test is quite similar as a real demand. Such test-induced failure/stress may cause the malfunction of equipment later or directly shorten the lifespan of product [192]. For production system, test may serve as cleaning and lubrication to rotating equipment thus slightly improve the reliability performance. The other advanced properties include human errors during maintenance activities [193] and the imperfect test [194]. These advanced properties can be modelled by introducing new states that represent the induced degradation and damage and the transitions attached with deterministic delay are assumed to reach such new states. Generally, the advanced properties of test and maintenance are deliberately removed from analysis for the sake of simplicity. For subsea system, these side-effect may have cumulative impact (i.e. sojourn time on the defined new state) on system availability and production as the result of lacking cost-effect means to remove them.

- **Non-constant rate of transition, *F***

Some components installed in subsea module remain untouchable or cannot be retrieval due to limited accessibility. Such components are assumed to have the non-constant (often increasing) failure rate, implying that need of other probability distributions like Weibull and Normal distribution.

- **Decoupling between deterministic events, *T, R***

This refers to the situation that test events and repair events are no longer sequential dependent. In practice, the maintainability is directly or indirectly compromised by architecture constraints, spare resources and accessibility. For subsea systems, the time to prepare repair crew and spare parts and associated mobilization is considerable (e.g. more than three months). Such delay is not negligible compared to the intervention interval (for rotating equipment may be five years or less). This situation requires other means to compensate for system availability and production, such as degraded mode of operation. The case study in section 6.4 model the compensating scenario that consists of two events: ‘faulty equipment is isolated’ and ‘system continue the production in reduced (but acceptable) level until maintenance vessel reaching the station’. States transition

formalism can account for such 'untrue' independence, however, with some limits.

Compared to safety systems operated in low-demand mode (i.e. demand for safety function is less than once per year), test and maintenance of production systems operated in continuous mode lead to the considerable downtime. This situation requires to find test and maintenance strategy with best cost/benefit ratio in terms of induced downtime and improved availability. The possible strategies include condition-based maintenance, inserted tests, postpone and reschedule of maintenance (as elaborated in section 5.4). Modelling such decoupling between events requires that the transition is conditioned/guarded on other states instead of sequence or scheduled time.

- **Multiple flow propagation, *F*, *T, R***

The modularization is generally assumed for new subsea design, such as SGB. The processing of hydrocarbon product is realized by critical processing equipment located at different modules of SGB, but the retrieval-based replacement only involves components located at the same module. Therefore, at least two information flows are considered. One is the state for each component, which is used for maintenance decisions. Another is the information flow to indicate how the required function is compromised by the change of component state. The case studies presented in section 5.4 and section 6.4 both have encountered this problem, where *measurement uncertainty* and *production deficiency* are assumed to be dependent on the number of functioning USM and the mode of operation, respectively. The solution is to introduce variables that can be updated by transition between states, thanks to the mechanism of predicates and assertion offered in SPN.

8.2.3 Modification to selection scheme of RAM modelling formalism

Figure 8-4 presents a formalized guideline to choose from formalisms presented in section 8.1, given the questions presented on the left side. From left to right, the expressiveness of modelling formalism is increased thus the simplicity is decreased (i.e. less concise, less readability and more resource-consuming for simulation and calculation even with powerful software). The number of entry point to modelling formalisms can be seen as a crude indication of flexibility in use.

The guideline starts from the identification of scenarios to be modelled, which can be completed following the instruction presented in the previous subsection 8.2.2. The formulated scenario enters into 'the checklist of ignored scenarios' (the

bottom left corner of Figure 8-4) when the associated stochastic description is missing in the early design phase. This implies the need of failure rate prediction and/or other means to obtain associated data. The formulated scenario can be also deliberately ignored, primarily under the practical considerations that there lacks the competence and software tools to support the modelling formalism with more expressiveness. The checklist can be used in the communication with system designers to register the limitations (i.e. risk) of RAM modelling.

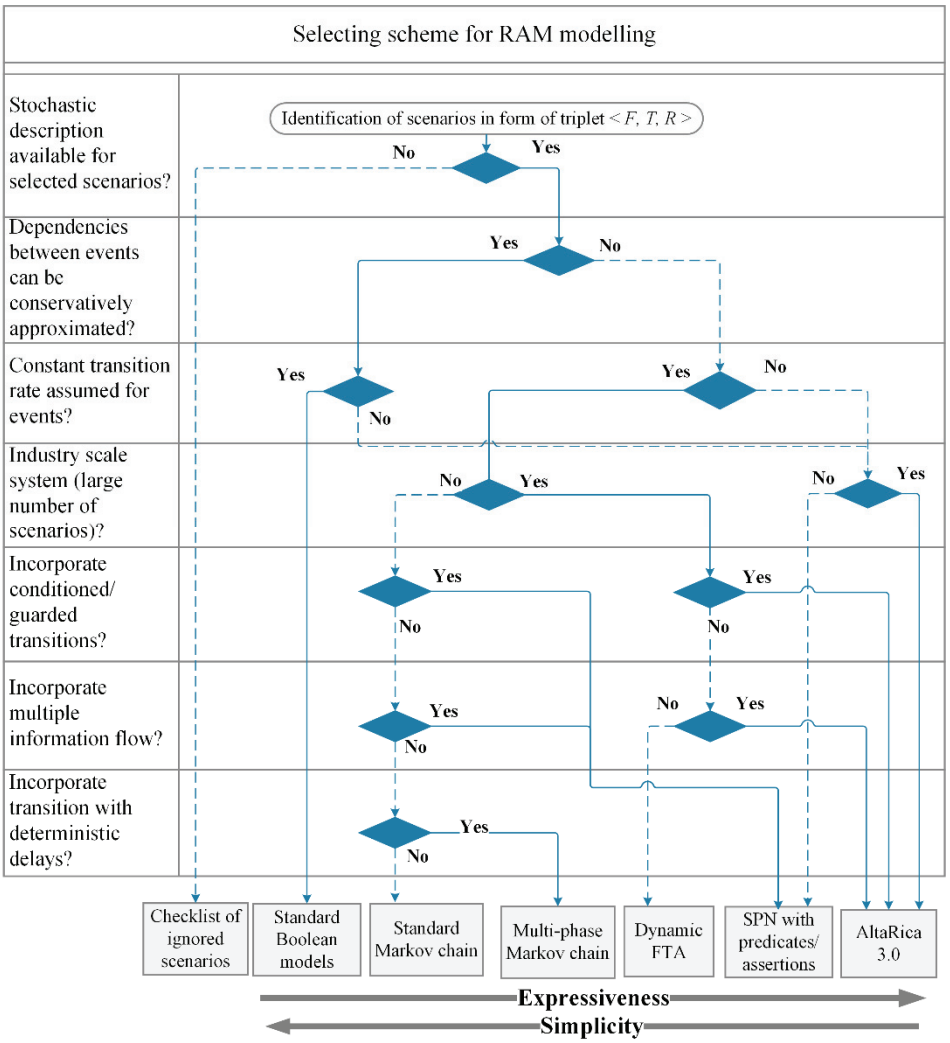


Figure 8-4 The proposed guideline on selecting modelling formalism

No case study is provided for the new guideline illustrated in Figure 8-4. Instead, the evaluation of the proposed guideline can be done by comparing to the existing guideline in ISO/TR 12489 [9]:

- **Remove the ambiguity of selection criteria:** the subsection 8.2.1 formalizes the definition of states, transitions and events. The nature of transition (i.e. random, deterministic and guarded) is used to formulate selection criteria (i.e. the questions presented on the left side of Figure 8-4). Therefore, it contributes to remove the ambiguity of selection criteria in the guideline of ISO/TR 12489 [9].

- **Consider plant-specific aspects:** rather than focusing on dynamic features encountered in safety system (e.g. staggered testing and periodic test), the subsection 8.2.2 discusses specific scenarios of relevance in a subsea context, e.g. delayed and postponed maintenance due to limited accessibility, reconfiguration and the like. In addition, the different states of the subsea processing and production equipment are assumed to have different impacts on required functions (e.g. operation, production and maintenance). This implies the need of introducing variables that represent the multiple information flow, which can be updated along with the state variables. As concluded in Figure 8-4, only SPN with predicates and assertion and AltaRica 3.0 can account for flow variables. In O&G industry, the commercial software like Maros and Taro [195] based on discrete event simulation can also suffice for this purpose. It is possible and interesting to seek for opportunities of a cross fertilization between them.

- **Enlarge the scope of candidate formalisms:** In addition, the scope of candidate formalism is increased by adding dynamic FTA and AltaRica 3.0. Dynamic FTA is comparable with Markovian model in term of expressiveness, but more suitable for industry case as the time to analyze is rather short. AltaRica 3.0 is a bit more expressive than SPN, and it facilitates the model construction for large scale system.

- **(Can be) used for generic system type:** The proposed guideline has been tailor-made for new subsea design. It be adapted for other industry sectors, if the modelling assumptions defined in subsection 8.2.2 are judged to be relevant.

Chapter 9 Review of RAM allocation models

As shown in RAM-SE framework, RAM requirement formulation is as the 'gate keeper' of RAM analysis. It embeds confirmation 'upwards' against overall targets and functional requirement obtained from operational analysis, and verification 'downwards' against the obtained quantitative indicators from RAM modelling. The process of formulating RAM requirement consists of two parts: one is *RAM specification*, to identify the overall requirements at *system-level*; another is *RAM allocation*, to define and distribute the system-level RAM requirements at *component-level*, given various criteria (e.g. costs of reliability improvement, complexity). This chapter is to review the state of art models used for RAM allocation and evaluate their suitability in new subsea design.

This chapter starts with clarifying the process of RAM specification. Then, it proceeds to review the mainstream RAM allocation models, and evaluate for application for subsea and early design evaluations. This chapter finally ends with recommendations on and directing future research in this topic.

9.1 RAM specification: procedure and content

RAM specification is an extension of the system or equipment *design specification*, with focus on the RAM related requirements. An important attribute of the RAM specification is to cover functions, beyond those being "obvious" from designer's own analyses and specifications. Such additional functionality may relate to provision of information (e.g. monitoring of technical state), allowance for testing (e.g. remote and diagnostics), protection of equipment, and behavior upon fault conditions.

The ultimate goal of RAM analysis is to ensure that the system being studied can satisfactorily and reasonably meet the specification of RAM requirement. The RAM requirement can be qualitative, which is open to interpretation in design process, such as 'not a single failure can prevent the system from functioning'. The RAM requirement can also be quantitative, which is testable and measurable, such as 'the system failure rate is less than 10^{-9} per hour'. The RAM requirement for ultrasonic flow meter assembly (section 5.4.2) is in both formats: 'not a single failure on USM can require the retrieval for calibration and adjustment during 20 years' service'.

RAM requirement must be used in conjunction with the supplementary statements [196]. For reliability requirements, the supplementary statements can be operating and environment conditions and use profile to give the insights about

system reliability. Similarly, the quantitative measure for maintainability Mean Time to Repair (MTTR) should be specified in together with the statements on maintenance access and the provision of maintenance support planning.

Beyond the process to formulate requirements about RAM attributes, RAM specification should clarify the satisfaction criterion. The satisfaction criterion refers to the means to test, demonstrate and verify that the requirement is fulfilled by the system. Therefore, it could be the test of component in simulated environment or RAM analysis. In practice, no stakeholder will accept the product that is only verified by RAM analysis. Yet, in early design phase, RAM analysis suffices as a crude verification and its result can be used to plan and design the simulated test.

9.2 Review of RAM allocation models

When the current design cannot meet the specified RAM performance, designers shall prioritize the real potentials for improvement on components or subsystem through RAM allocation. RAM allocation here refers to a rational approach that assigns the RAM specification of each sub-assembly as a proportion of overall specification based on a given criteria, e.g. reduce failure rates of some failure modes and/or improve the procedure of repair and maintenance activities. RAM allocation is a crucial step in early design phase. For a design solution that may consist of over thousands of parts, it is impractical (sometimes even impossible) to verify whether the requirement is met when all parts are brought together. It is therefore necessary to presume a level of complexity given the structure and task of subsystem. As such, carrying out RAM allocation presumes to: (1) support guideline of directing engineering efforts, (2) reduce computational burden of RAM modelling.

A considerable number of models has been proposed for RAM allocation. The commonly used allocation models are reliability-based for the non-repairable system. The approaches include the equal apportionment method [197], Aeronautical Radio Inc. (ARINC) method [198], Advisory Group on Reliability of Electronic Equipment (AGREE) method [199] and the method based on minimum effort algorithm [197, 200]. Considering the importance of repair actions, some extensions are made to cover repairable system so that availability and maintainability can be allocated optimistically. In addition to top-down models (i.e. allocating system-level target), some bottom-up models that consider potential improvement of reliability on lowest level (e.g. failure rate reduction) are developed, see the work by Yadav and Zhuang [201]. Besides, more advanced models are proposed based on complex optimization algorithm and dynamic programming, see also the annotated review article by Kuo and Wan [202].

From literature, it does not seem that these advanced models are widely adapted as they are too complex and often resource-consuming. As pointed out by Amari and Hegde [203], RAM allocation must be fast and easy to implement, by assessing the information and constraints of interest from RAM point of view when deciding on conceptual solution for system and its subsystem. Given this consideration, some simple and intuitive RAM allocation models have been proposed, e.g. the availability allocation model based on minimum effort algorithm proposed by Jigar et al. [204] and reliability and maintainability allocation models proposed by Vintr et al. [205].

The mainstream allocation models for reliability of non-repairable system, maintainability and availability of repairable system are summarized on basis of [206] in the following Table 9-1, Table 9-2 and Table 9-3. The main principle and assumptions of each model are briefly discussed. The underlined and bold text is used to indicate the **required information inputs** for each model, in addition to the basic information (e.g. system-level RAM requirement and system structure).

Table 9-1 Reliability allocation models for non-repairable system

Model	Description	Principle and inputs
Equal apportionment model [197]	Assuming that the system S consists of a series of n independent and non-repairable subsystems i assigned with same weight w_i The reliability of system is expressed as $R_s^* = (R_i^*)^n$	It is assumed that reliability requirement of component is equally distributed. **No additional input information is required.**
ARINC model [197],[198]	Assuming that a system S consists of a series of n independent and non-repairable subsystems i assigned with weighted failure rate, $\lambda_i^* = w_i \lambda_S^*$ where the weight equals to $w_i = \frac{\lambda_i}{\sum_{j=1}^{n} \lambda_j}$	It requires **failure rate** for obtaining allocation weights
Extension to ARINC model [207]	Assuming that a system S consists of a series of n independent and non-repairable subsystems i assigned with weighted failure rate,	It requires **failure rate** for obtaining allocation weights, and the weight is adjusted by **safety margin** (assigned by designer)

	$\lambda_i^* = w_i \lambda_S^*$, where $w_i = K\left[a\frac{1}{K} + (1-a)\frac{\lambda_i}{\sum_{j=1}^{n}\lambda_j}\right]$ K is safety margin to allow for design changes and a is the weight used in equal apportionment model	
AGREE model [197],[199]	Assuming that a system S of m modules and module i has n_i components, where $\lambda_i^* = -\frac{n_i \ln[R_s^*(t)]}{\omega_i t_i \sum_{i=1}^{m} n_i}$ ω_i is the probability that system fails when module i has failed.	It requires the **complexity of system (i.e. the number of components)** for obtaining allocation weights
Approaches of assessing factors that influence failure rate [208],[209],[210]	Assuming that there is a p number of RIF ($RIF_{i1}, RIF_{i2,\ldots} RIF_{in}$) for the component I, The weight is assigned as $w_i = \frac{f(RIF_{i,p})}{\sum_{i=1}^{k} f(RIF_{i,p})}$ where $f(RIF_{i,p})$ denotes the influencing function of RIF on component i	When required failure rate to ARINC model is not available, using the **reliability influencing factors** to estimate the failure rate
Minimum effort algorithm model	(1): Consider $R_1 \le R_2 \le \ldots R_n$, after allocation the system satisfies $(R_0)^k \prod_{j=k+1}^{n} R_j = R_S^*$, assuming efforts function is the same for all components. Where k is determined when $R_{0,j} = \left(\frac{R_s^*}{\prod_{i=j+1}^{n} R_i}\right)^{\frac{1}{j}} \ge R_j$ and $R_{0,j+1} = \left(\frac{R_s^*}{\prod_{i=j+2}^{n} R_i}\right)^{\frac{1}{j+1}} \le R_{j+1}$ (2) Assuming that effort function is not the same for components, where	The main assumption is that the effort to improve low-reliability components is less than that of the effort to improve high-reliability components. **The order of component reliability is required as input.**

	denotes $E_i(R_i, R_i^*)$ as efforts for component *i*. The optimization is therefore: $\begin{cases} \min \sum_{i=1}^{n} E_i(R_i, R_i^*) \\ h(R_1^*, R_2^*, ..., R_n^*) \geq R_s^* \end{cases}$	

Table 9-2 Maintainability allocation model

Model	Description	Principle and inputs
Equal apportionment-based model [211]	Same principle as that of reliability allocation. Assumes $MTTR_i$ is same for all components	The main assumption is that the repair action is immediately performed after failure is revealed. **No additional input is required.**
Failure rate complexity method (FRCM) [211]	The mean repair time of a system *S* is expressed as $MTTR_S = \frac{\sum N_i \lambda_i MTTR_i}{\sum N_i \lambda_i}$ where $MTTR_i = \frac{\lambda_H}{\lambda_i} MTTR_H$, λ_H denotes the highest failure rate	The main assumptions are (1) the repair action is immediately performed after failure is revealed (2) the highest **failure rate of component** demands lowest repair time
Approaches of assessing factors that influence repair time [212]	Similar as that of reliability allocation. The weight of component *i* is $w_i = \frac{\lambda_{avg,i} k_i}{\lambda_i k_{avg,i}}$, where $k_i = \sum_j^m k_{ij}$ is the weight coefficient of factor *j* in unit *i*	The main assumptions are (1) the repair action is immediately performed after failure is revealed (2) the maintainability (i.e. MTTR) of component is subjected to **influencing factors (e.g. accessibility, scalability, testability)**

Table 9-3 Availability allocation model

Model	Description	Principle and inputs
Equal apportionment-based model [213]	Allocates the equal failure rate for a given availability target.	The main assumption is that only the effort to improve reliability is required. **No additional input is required.**
ARINC-based model [213]	Reduces subsystem failure rates by equal percentages such that the failure rate goal is reached.	The main assumptions are that (1) only the effort to improve reliability is required, and (2) equal effort is required to reduce **failure rate** by equal percentage of failure rates.
AGREE-based model [213]	The weight of component ω_i indicates the criticality of the component functionality.	The main assumptions are that (1) only the effort to improve reliability is required, (2) considers **the percentage of the time the functionality** of each subsystem is used for allocate reliability (also called duty cycle by engineers)
Amari and Hegde [203]'s model	Meeting system availability requirements requires efforts in reducing failure rate and increasing repair rate	The main assumptions are that (1) the effort to improve low-availability components is less than that of the effort to improve high-availability components (2) considers **engineering efforts** (labor, time, costs) for improving availability
Jigar et al. [204]'s model	(1) identical improvement cost/complexity function (2) varying cost function (3) complexity-constrained optimization	The main assumptions are that (1) the effort to improve low-availability components is less than that of the effort to improve high-availability components (2) considers **cost and complexity (i.e. the number of components)** for improving availability
Barabady and Kumar [214]'s model	Considers the availability importance of component *i* in a system of *n* components $I_A^i = \frac{\partial R_s(t)}{\partial R_i(t)}$	It requires **failure rate and repair rate** to obtain the importance measures.

9.3 Evaluation of existing RAM allocation models

Each allocation model may have their own strength and weaknesses, and can be of interest to evaluate their suitability in a subsea context. The modularity of subsea system is foreseen as an important issue in allocation model. The case system SGB (introduced in section 2.3) is considered as example. The objective of pursuing modularity in the SGB design is to improve the maintainability and scalability of each functional modules that operate wells. As illustrated in Figure 9-1, the shell of SGB provides the stabilization to withstand the dynamic loads created by the currents on the seabed. The compartments host the functional modules through coordination, e.g. communication bus, signal processing, interconnectivity. The modular design saves the installation and intervention cost by reducing overall weight and size, and add flexibility on meeting well requirements.

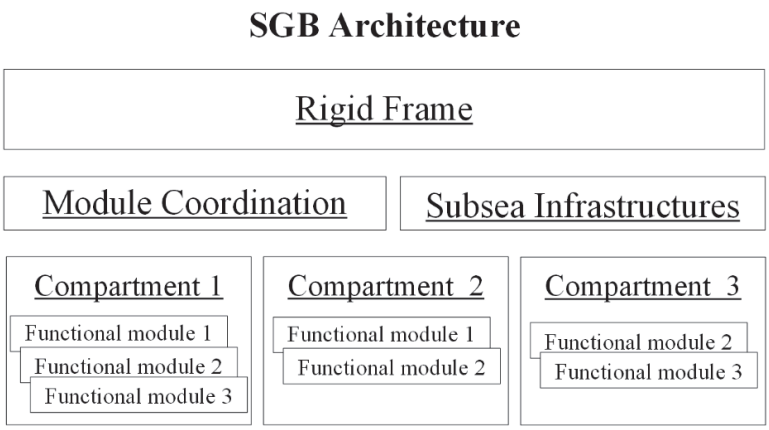


Figure 9-1 Modularity of SGB

Applying allocation models for the modular system may be challenging, due to the possible functional and architecture *dependencies*. The module may share the working load (through bypassing) and utility (e.g. electric power and hydraulic power), meaning that the unreliability of module may have different acceptable disturbance on the required system availability. The assumption on series-parallel system structure is therefore no longer valid. Solving this problem relies on a good algorithm to define the dependencies mathematically. Some initiatives have proposed to transfer the modularity problem to segregation constraints [215]. Yet, the proposed model is too complex and resource demanding to be applied in early design phase where the design is not definite. The future research arena can be to finding a user-friendly RAM allocation model that accounts for modularity problem.

Another research direction can be on the maintainability allocation model. The models presented in Table 9-2 generally assume that repair action is immediately performed or initialized after the failure detection. This assumption may not be valid in the case of subsea design where the advanced maintenance strategies are implemented, such as group-maintenance and delayed maintenance. It can be interesting to account for the time-characterized repair actions.

Finally, it is important to investigate on subsea-related factors that affecting the *efforts* of improving a component's RAM performance. The efforts can be interpreted according to engineering contexts, such as costs for material that offers better reliability performance in the stated conditions and the easiness (e.g. time) for reliability and availability improvement. The effort can be transferred into *cost function*, then the allocation is to minimize the total costs for RAM improvement. The appropriate assessment for obtaining cost function can be critical to RAM allocation model, especially when engineers have not enough information and experience of technologies implemented subsea. Trying to capture all relevant factors is an impossible task. Instead, based on the reflections from subsea complexity (subsection 3.2.2) and discussions about modelling scenarios (subsection 8.2.2), some evident factors are listed in Figure 9-2. The general concept of RAM requirement consists of two parts (i.e. MTTF and MTTR), and they can be divided into understandable quantities. The contributing factors related to reliability requirements (e.g. minimum required MTTF) and maintainability requirement (e.g., maximum allowed MTTR) are summarized as shown. Figure 9-2 itself is open for further refinement, and its interpretation by system designers and associated indexing can be important elements in the communication and joint concept analysis under RAM-SE framework.

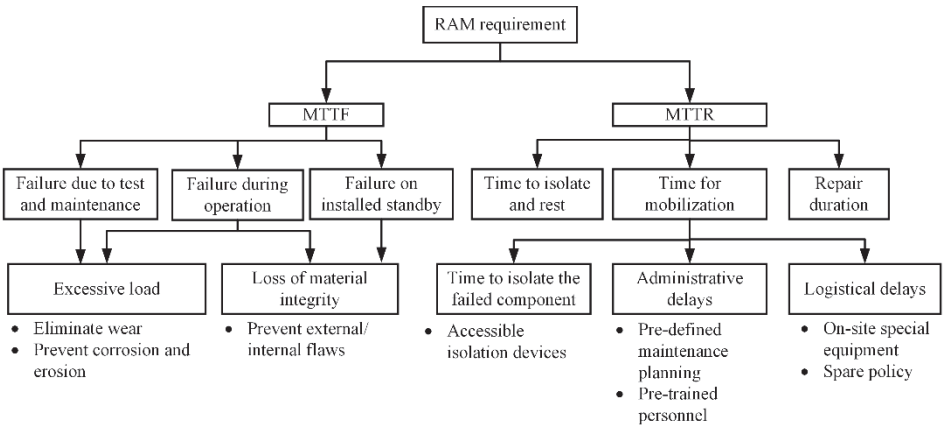


Figure 9-2 Factors to be considered in allocation model of subsea design

Chapter 10 Summary of main results & future works

Incorporating an efficient RAM analysis in the early phase of new subsea design has been the main focus of this thesis. This chapter is firstly to summarize the contributions of main results under the formulated problems and objective in section 1.3. Then, the future works regarding the extensions to the current results as well as the applications for industry practices are described.

10.1 Summary of main results

This thesis is primarily meant complementary to the existing standards and practices that reach their limits in the early phase of new subsea design, for instance, IEC 60300 [10], DNV-RP-A203 [15] and ISO/TR 12489 [9]. In this research project, the initial problem was the novelty and complexity of subsea systems. They are recognized as two main aspects that influence the process and quality of RAM analysis. The specific considerations are derived for the main objective that was to synchronize RAM analysis to the subsea design process and enable its efficient use in early trade-off about maintenance strategies, system configurations and the like.

This thesis involves a variety of interdisciplinary models and theories, as well as a set of existing models but from a subsea insight. The main deliverables describe improvements and modifications towards six main steps of RAM analysis (section 4.2). The detailed contributions are summarized as follows.

- **RAM-SE framework**

This work is mainly associated with *system familiarization* and *design review and recommendations* in RAM analysis.

Subsea design involves many specialty disciplines and groups, a structured means for coordinating the contributing efforts is needed. SE[11] is recommended for subsea design based on this vision. RAM is a subfield of SE, however, the inter-link is gradually lost as RAM analysis become more dedicated and specialized. In this respect, two expertise domains are assumed in a subsea design process: one represents the elaborations from engineering design teams, the other represents the elaborations from RAM analysts. While these two expertise domains focus and contribute to the same subsea design, they have different expertise and expectations. The evaluation of their used concept and produced

[11] Systems Engineering

models has shown that the interface between these two expertise domains is indispensable and possible.

RAM-SE framework is proposed to unify the elaborations from these two expertise domains and describe how the interface should be. For RAM analysts, the construction of RAM models conforms to a suite of SE model developed in design analysis, which reduces the risk of working from an inconsistent and incorrect system concept. Then, system designers can correctly capture the indications and recommendations derived from RAM models conducted in a systematic and iterative manner.

The design proposal of subsea ultrasonic flow meters is used to demonstrate the RAM-SE framework. Although the case study is quite restrictive and simple, it has demonstrated how RAM analysts appreciate the efforts by system designers and vice versa. The high-level considerations and needs from system designers were reflected in the associated RAM requirements. Given the formulated RAM requirements, six design alternatives were proposed with respect to different system configurations and maintenance strategies. They were evaluated by RAM modelling. The cost estimation in terms of operational and maintenance costs and produced values suggests that only one design alternative enters into detailed design phase for further refinement.

The main contribution of RAM-SE framework is evaluated from direct and indirect perspectives. The direct contribution, that is for RAM-SE framework itself, which organizes the force of the two expertise domains as early as possible, by removing potential misconception and misunderstanding arisen from heterogeneity between the two expertise domains. It should be noted that, although this thesis emphasizes on the early phase for subsea design, the proposed framework can be applied in different works (e.g. other industry sectors) and other contexts (e.g. other stages of system development).

There are also indirect contributions. RAM-SE framework presented in Chapter 5 can serve as a baseline to improve, guide and generate RAM models. Two examples are dedicated in this thesis. First, the core concept of SE, systems thinking, is employed in STPA used for *dysfunctional analysis* (section 6.2). It can be seen as the cross-fertilization of SE and RAM. Second, the produced SE models are helpful for *RAM modelling*, because they helps to generalize modelling issues thus the model construction is faster and easier (subsection 8.2.1).

- **STPA-RAM modelling**

This work is mainly associated with *dysfunctional analysis* and *RAM modelling and calculation* in RAM analysis.

Subsea systems have become increasingly intelligent, where the computer-based control is used to implement a majority of the functionality. The failure behaviors arisen from complex and software-intensive interactions must be characterized and understood as early as possible. STPA [12] is chosen for dysfunctional analysis based on this need. STPA can identify more failure behavior (i.e. the candidate for modelling) compared to traditional models like FMECA, thus it reduces uncertainty associated with completeness of RAM analysis. Yet, STPA abandons the probability aspects, which in turn increases the difficulty in interpreting its results in communication stage of RAM-SE framework.

In this respect, an integrated approach that combines the STPA and RAM modelling through stochastic Petri-nets model is proposed, denoted as STPA-RAM modelling. The main approach is to convert potential loss (hazardous) scenarios identified in an STPA into state automata, thus it can be complied into SPN model that follows state-transition formalism. RAM modelling can be used to stochastically describe the context for each control action. In the case study, it has been shown that the STPA-RAM modelling can quantitatively assess the failure behavior that impact on system production, maintenance and emergency management.

The main contribution of STPA-RAM modelling is twofold. From the dysfunctional analysis point of view, this work depicts a standard procedure for characterizing and quantifying the hazardous scenarios associated with the engineering systems and the outer controller loops. This work helps to clarify to what extent STPA can contribute to decision-making in an engineering design. From the RAM modelling point of view, the control structure offered in STPA helps to construct the pattern-wise SPN model. It means that the time to construct SPN is saved and the readability is increased a bit for analysts who master STPA.

The major limitation for STPA-RAM modelling is the size of model. Only a limited number of loss scenarios is considered in the same model, which makes the proposed approach less appealing for industry-size systems. In addition, the current proposal did not account for non-statistical factors like pressure changes

[12] System theoretical process analysis

in reservoir. The combination to the physical model with real-time simulation is beyond the scope of this work.

- **BN-based failure rate prediction model**

This work is primarily associated with *failure rate prediction* in RAM analysis.

Using RAM analysis in the qualifications of new technologies or existing technologies installed in new environments rely on access to critical reliability parameters like the failure rates. The failure rates builds on prediction models, that incorporates previous experience (of same or similar technologies or use) and design analyses. Many models for failure rate prediction have been proposed, such as [82, 83]. They reach their limits in early design phase, such as and lack of means to incorporate data uncertainty, or fails to account for dependencies among operating and environmental conditions. Bayesian Networks (BNs) are examples of models that can be constructed very early with requirements ("nodes") of data that is important for failure rate prediction. One advantage of BN is the ability to represent conditional probabilities, i.e. flexible inclusion of reliability influencing factors that may have an impact of the parameters of the failure rate model given certain pre-conditions. Another advantage is the possibility to update the conditional probabilities, when new knowledge is added (at different stages of the design and later in operation). As part of this PhD research, an illustrative case is used to demonstrate a BN-based model in the early design phase. It has been shown that BN-based failure rate prediction model that can be well suited for selecting monitoring needs in the early design phase as well as building confidence in the prediction along with the maturing of design concept.

This work is not evaluated as the *new* model for failure rate prediction, considering that the author does not contribute to develop new algorithms to determine the selected RIFs and associated influencing function. The main contribution is therefore to explore the possibilities and capabilities of BN on how to handle unfamiliar failures or known failure, with the best knowledge and information at hand. The BN-based failure rate model removes some restrict assumptions on selecting RIFs and enables the uncertainty considerations, to provide an 'approximate but more closed to reality' estimation in the early design phase. In addition, the confidence in the predicted failure rates relies also on facilities available to carefully monitor the performance during continuous operation. Models for failure rate prediction must match the availability of data, but the availability of data can be influenced by how the system is designed. This is also why BN-based failure rate prediction is placed in RAM-SE framework: to put enough attention to the specification of design requirements that allow

adequate gathering of data about technical condition, operating environment, results of testing, and technical failures.

- **Guideline of RAM modelling**

This work is primarily associated with *RAM modelling and calculation* in RAM analysis.

Many formalisms are available for completing RAM modelling and calculation. They are different in terms of easiness of construction, model readability, flexibility, and expressive powers. It is argued that the expressiveness of modelling formalism is traded for less readability and more complex model structure. They are chosen at different stages and for different system complexity characteristics. The existing guideline provided in ISO/TR 12489 [9] is primarily used for safety system, which does not suffice for subsea production and processing system that are assumed to be multi-state and multi units.

This work consists of two parts. The first part is to review and carry out a comparative study of commonly-used formalisms. The second is to discuss how to make a smooth transition between system specifications and RAM modelling. It is sometime error prone for RAM modelling when static structure and dynamic behavior have not yet been specified to a sufficiently detailed level. Then, it proceeds to discuss the own modelling challenges of subsea processing and productions, and generalize a set of assumptions that can be judged by the model designers. The result is the new guideline to choose the adequate modelling formalism, considering the trade-off between expressiveness and simplicity. The advantages over the existing guideline provided in ISO/TR 12489 [9] have been summarized in section 9.3, for instance, removing ambiguity of selection criteria and adding sector-specific considerations.

The main contribution of this work is to provide a better picture of candidate formalisms used for modelling subsea production and processing system as well as safety system. There is no a single formalism can fulfill every purpose of RAM modelling alone. The proposed guideline gives RAM analysts a good chance to evaluate the convenience and loss by using selected formalism. This work also contributes to address the efforts that have been made by system designers in RAM modelling (through RAM-SE framework), so that system designer can systematically judge or make a judgement about confidence of RAM modelling in the related decision context.

- **A review of RAM allocation models**

This work is primarily associated with *RAM specification and allocation* in RAM analysis.

RAM specification is to document the non-ambiguous and testable RAM that a system should satisfy. The quantitative RAM requirement, such as MTTF and failure rate, can be allocated crudely to the lower-level system structure through the defined constraint. This is crucial step in early design, to restrict the scope of RAM analysis and direct the engineering efforts if RAM improvement is required.

This work is to carry out a review on mainstream allocation models and evaluate their uses in subsea design cases. Both traditional and newer models has been benchmarked against key design attributes of subsea systems. Three future directions are identified: (1) to derive the modularity as the constraint in allocation model, (2) to consider the time-characterized maintenance actions in allocation process, (3) to systematically investigate the relevant factors for RAM improvement from engineering (e.g. manufacturer) perspective thus the cost function in allocation models can be confidently assigned.

The main contribution is to indicate in which areas the author recognizes the benchmarking in face of subsea systems, and prioritize the future efforts among researchers to battling the difficulty of applying allocation models for subsea design.

10.2 Recommendations for future work

This thesis, like any others, is not exhaustive. There are many subjects left to think about and solve for RAM analysis in early design, and this doctoral contribution itself evokes a few questions to direct future directions. Here the future work is divided into short-term that is for methodological standpoint, as well as long-term that is for improving industry practice.

10.2.1 Short-term future work

RAM-SE framework provided in this thesis represents the first step to union SE domain and RAM domain, not the final one. The process described by the RAM-SE framework is highly simplified and idealized. RAM-SE framework only restrictively discusses interlinks between these two disciplines in light of models with high acceptance and commonality in each community, e.g. the models used in SysML. It will give more values and refinement of RAM-SE framework if other types of SE models to RAM practice are investigated. Another possible future work is to develop supporting tools for communication stage and joint concept analysis stage, such as a graphical navigable model for visualizing

interactions between RAM models and SE models. Some works have been done for automatically transferring SysML models into RAM models such as Markovian models or SPN model. Yet, few is done conversely, to our best knowledge.

For STPA-RAM modelling, the most urgent improvement is to develop suitable approach for processing STPA results, i.e. to screen out and prioritize the loss scenarios. One possible strategy is to evaluate the effectiveness of safety constraints in terms of its availability and easiness of implementation, as well as the criticality of associated losses. This may require not only the advance in the analytical method that assign criticality, but also the multidisciplinary participations for conducting STPA to seek multiple perspectives for prioritization. The similar work has been carried out internally in the RAMS research group of SUBPRO [41]. Another future direction is to evaluate the background knowledge and sensitivities of assumptions made for probabilistic models, so the confidence of results can be judged by decision makers. Some approaches have been discussed in [152]. The next step is then to fuse it into the procedure of STPA-RAM modelling.

For BN-based failure rate prediction, one future direction can be relevant to test if this model can be implemented in combination with condition monitoring and measurements provided by sensor systems subsea. In this respect, the need of continuous monitoring is increased, but it must be balanced to the added complexity and costs of introducing equipment for monitoring purposes. Another research direction could be to collect other types of evidence can be used to update the estimation of failure rate. The occurrence of failure features low frequency in subsea environment. It is interesting to discuss how to use the historical failure rate from similar sectors like chemical processing plant onshore. Therefore, BN-based model also relies on other 'reliable' data from other sectors, as long as that the relevance between sectors is judged and evaluated in BN model.

For the guideline on RAM modelling, the future work is naturally to expand the scope of investigated modelling formalisms so the guideline can be used for generic types of *system*. The candidates are for example colored Petri-nets and timed automata, which have not been widely used in O&G sector or process industry in general. It can be interesting to investigate in which cases they are required to ensure the expressiveness of RAM modelling. For instance, timed automata can be used to capture continuous phenomena of events.

For the review work of RAM allocation model, the future steps for this research have already been given and discussed.

10.2.2 Long-term future work

One remaining work can be to integrate the proposal into adopted industry practices and evaluate its practical values. This type of future work is regarded as long-term, as it would take years or even decades to truly make a difference or observe remarkable improvements.

All the contributions are evaluated from a methodological point of view, with relatively simple cases with simplified engineering context. Unfortunately, there has been insufficient time and chance to apply the complete collection of methods from this research onto one single industrial case which could be followed from the initial specification to the prototyping and final installation. The feedback from how the new contributions could benefit decision-making in the early design phase cannot be fully confirmed until the new system has been installed and operated for some time. This may be a starting point for future research topics in the qualification of new subsea technologies: To evaluate the suitability and possibility for improvement of RAM analysis methods considering the feedback (lessons learnt) from how well they supported decisions that led to reliable systems in operation.

In this respects, the proposal can be implemented in existing TQP practice of O&G industry, for example DNV-RP-A203 [15]. TQP is to convince the operator that the new product is fit for use and has sufficient reliability and availability. The important parts of TQP include dysfunctional analysis (also called as 'threat assessment' in TQP), failure rate prediction, and RAM modelling (also called as 'performance assessment' in TQP), which are aligned with the topics investigated in this thesis. The proposals here can be seen as good alternatives for methods documented in DNV-RP-A203 [15]. For instance, DNV-GL is also looking for the opportunity of applying STPA for software-intensive system [147]. Yet, the efforts must be paid to make the related proposals to be simply practical and user-friendly. STPA-RAM modelling approach can be easily encoded into the formal language like AltaRica 3.0, or more commonly-used one like Matlab. The automatic process for generating loss scenarios graphically and compiling into SPN models is considered as the key enabler for its practical and commercial use.

It may be of interest to consider other sectors to enrich the content of this research work and hopefully bring ideas for transfer of knowledge from this work to other domains of interest. For instance, the aviation industry is considering introducing STPA in its procedure of safety assessment. The extension made in this PhD work (i.e. STPA-RAM modelling) is therefore relevant.

Though modesty is a virtue, one ambiguous goal however is that this doctoral contribution will be a new way of using RAM analysis in industry. Most O&G

companies approach RAM as conformance by a group of specialists, but the gate keeper of subsea design are discipline engineers that are not familiar with reliability theory and practices. This issue may be relieved by involving experienced engineers, however, it will never extinct by doing so. Applying RAM-SE framework is foreseen to result in a significant gain especially in big projects, in terms of saving time and costs for design iterations, model validation and the track of specification revised frequently.

10.3 Closing remarks

In the very beginning of this PhD project, I was asked to provide some RAM suggestions and recommendations for the design of subsea gate box that was at very preliminary stage. The designer of subsea gate box and I (as a young and unexperienced RAM analyst) explained both our needs and concerns, to support our own disciplinary analyses and decision-making. I experienced that it was difficult for me to formulate my needs for input and also how to utilize the results of RAM analysis in combination with analyses already made by the designer. I experienced the process of interaction was influenced by having different background knowledge, 'dialogues' and jargons. At the same time, I learnt how important it is to always strive to understand the designer's perspective, and not carry out the RAM analyses in isolation. This first bad 'consultation' experience reminded me the importance of proper means for communication between different disciplines, and how difficult and challenging it can be. At the same time, it gave be a very good starting point for this research work. Now, when I have reached the end of this PhD project, I hope that others find my contributions useful and necessary to avoid what was my first experience.

Reference

[1]. Kuhnle, T.I., *All subsea – creating value from subsea processing* in *DNV GL strategic research & innovation position paper* 2015, DNV GL.

[2]. Ruud, T., Idrac, A., McKenzie, L.J. and Høy, S.H., *All Subsea: A Vision for the Future of Subsea Processing*, in *Offshore Technology Conference*. 2015, Offshore Technology Conference: Houston, Texas, USA.

[3]. Økland, O. and Ramberg, R.M., *Subsea Factory–Standardization of the Brownfield Factory*, in *Offshore Technology Conference*. 2015, Offshore Technology Conference: Houston, Texas, USA.

[4]. Ramberg, R.M., Davies, S.R.h., Rognoe, H. and Oekland, O., *Steps to the Subsea Factory*, in *Offshore Technology Conference*. 2013: Rio de Janeiro, Brazil.

[5]. Equinor. *https://www.equinor.com/en/where-we-are/norway/asgard-subsea-gas-compression.html*. 2018.

[6]. OG21, *TTA4-Future technologies for production, processing and transportation*. 2015, Norway: OG21.

[7]. ISO 8402, *Quality Vocabulary*. 1986, Geneva, Switzerland: International Standards Organization.

[8]. IEC 60500-191, *International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*. 1990.

[9]. ISO/TR 12489, *Petroleum, petrochemical and natural gas industries -- Reliability modelling and calculation of safety systems*. 2013, Geneva: International Electrotechnical Commission.

[10]. IEC 60300, *Dependability management*. 2003, Geneva: International Electrotechnical Commission.

[11]. Stapelberg, R.F., *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*. 2009, London: Springer.

[12]. IEV-192, *Dependability* 2015: International electrotechnical vocabulary.

[13]. IEC 60300-3-1, *Dependability management Part 3-1: Application guide Analysis techniques for dependability –Guide on methodology*. 2003.

[14]. ISO 20815, *Petroleum, petrochemical and natural gas industries– Production assurance and reliability management*. 2008, Geneva: International Organization for Standardization.

[15]. DNV-RP-A203, *Qualification of New Technology*. 2011, Høvik, Norway: DNV.

[16]. API-RP-17N, *Recommended Practice Subsea Production System Reliability and Technical Risk Management*. 2009: American Petroleum Institute.

[17]. ISO 13628-1, *Petroleum and natural gas industries - design and operation of subsea production systems*. 2005: International Organization for Standardization.

[18]. NORSOK U-001, *Subsea production systems. Edition 4*. 2015.

[19]. SAE ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. 1996, USA.

[20]. EN50126, *Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS)*. 1999.

[21]. W. Creswell, J. and L. Plano Clark, V., *Designing and Conducting Mixed Method Research*. 2011.

[22]. Kothari, C.R., *Research Methodology :: Methods and Techniques (Second Edition)*. 2004: New Age International Publishers.

[23]. Bai, Y. and Bai, Q., *Subsea Engineering Handbook*. 2010, Boston: Gulf Professional Publishing. xxv.
[24]. Ruud, T., Idrac, A., McKenzie, L.J. and Høy, S.H., *All Subsea: A Vision for the Future of Subsea Processing*. 2015, Offshore Technology Conference.
[25]. Roberts, C., Strutt, J. and Eriksen, C., *Building a Reliability Strategy for Subsea Systems Design*, in *International Conference on Long Distance Subsea Tiebacks*. 2001.
[26]. API-RP-17A, *Design and Operation of Subsea Production Systems-General Requirements and Recommendations*. 2011.
[27]. Aadland, A.-K. and Petersen, K., *Subsea All Electric*, in *Offshore Technology Conference*. 2010: Houston, Texas, USA.
[28]. Diaz, M., Stanko, M. and Sangesland, S., *Exploring New Concepts in Subsea Field Architecture*, in *Offshore Technology Conference*. 2018.
[29]. API-RP-17O, *Recommended Practice for Subsea High Integrity Pressure Protection Systems (HIPPS).* 2009.
[30]. Bai, Y. and Bai, Q., *Chapter 2 - Subsea Field Development*, in *Subsea Engineering Handbook*. 2010, Gulf Professional Publishing: Boston. p. 27-62.
[31]. Cunha, L.S., Felix, T., Meuter, P., Bourne, M., Fletcher, N., Vasconcellos, J.H. and Hollingsaeter, T.F., *Development and Qualification of a High Differential Pressure Subsea Pump*, in *OTC Brasil*. 2013, Offshore Technology Conference: Rio de Janeiro, Brazil.
[32]. Diaz, M., *Postdoc research plan- Subsea Gate Box*. 2015.
[33]. NORSOK P-001, *Process design (edition 5)*. 2006.
[34]. API-17F, *Specification for Subsea Production Control Systems (2nd edition)*. 2006.
[35]. NORSOK D-001, *Drilling facilities (3rd edition)*. 2012.
[36]. NORSOK Z-013, *Risk and emergency preparedness assessment*. 2010.
[37]. ISO 14224, *Petroleum, petrochemical and natural gas industries -- Collection and exchange of reliability and maintenance data for equipment*. 2016.
[38]. NOG-070, *Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry*. 2004, Norway: The Norwegian Oil and Gas Industry Association.
[39]. IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety related systems. Part 1-7*. 2010, Geneva: International Electrotechnical Commission.
[40]. IEC 61511, *Functional Safety – Safety Instrumented Systems for the Process Industry*. 2003, Geneva: International Electrotechnical Commission.
[41]. SUBPRO, *Subsea production and processing*. 2015: https://www.ntnu.edu/subpro.
[42]. Mankins, J.C., *Technology Readiness Levels: A White Paper. Technical report*. 1995, Washington, DC: NASA, Office of Space Access and Technology.
[43]. Homstvedt, G., Pessoa, R., Portman, L., Wang, D., Gonzalez, J., Maldancer, M. and Margulis, J., *Step-Change Seabed ESP Boosting*, in *Offshore Technology Conference*. 2015: Brazil 27-29 October.
[44]. Baker Hughes, *US patent 7565932: Subsea Flowline Jumper Containing ESP*. 2007.
[45]. Johansen, I.L. and Rausand, M., *Defining complexity for risk assessment of sociotechnical systems: A conceptual framework.* Proceedings of the Institution

of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2014. **228**(3): p. 272-290.
[46]. Årstad, I. and Aven, T., *Managing major accident risk: Concerns about complacency and complexity in practice.* Safety Science, 2017. **91**: p. 114-121.
[47]. Hollnagel, E., *Coping with complexity: past, present and future.* Cognition, Technology & Work, 2012. **14**(3): p. 199-205.
[48]. Edmonds, B., *Syntactic Measures of Complexity.* 1999.
[49]. Lloyd, S., *Measures of complexity: a nonexhaustive list.* IEEE Control Systems, 2001. **21**(4): p. 7-8.
[50]. Cilliers, P., *Complexity and post-modernism: understanding complex systems*. 2002: Taylor & Francis.
[51]. Hollnagel, E., Woods, D. and Leveson, N., *Resilience Engineering : Concepts and Precepts*. 2006.
[52]. Perrow, C., *Normal Accidents: Living with High-Risk Technologies*. 1999.
[53]. Vatn, J., *Can we understand complex systems in terms of risk analysis?* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2012. **226**(3): p. 346-358.
[54]. Strategos. *http://www.strategosinc.com/socio-technical.htm*. 2007 [cited 2018.
[55]. Sammarco, J., *A normal accident theory-based complexity assessment methodology for safety-related embedded computer systems, PhD thesis*. 2003.
[56]. O'Connor, P. and Kleyner, A., *Practical Reliability Engineering, 5th Edition*. 2012, Hoboken, NJ: John Wiley & Sons, Inc.
[57]. Zhang, J., Liu, Y. and Lundteigen, M.A., *Framing reliability specification in early design phase of subsea systems*, in *Proceedings of 23rd ISSAT International Conference on Reliability and Quality in Design*. 2017: Chicago, Illinois, U.S.a.
[58]. Murthy, D.N.P., Rausand, M. and Østerås, T., *Product Reliability: Specification and Performance*. 2010, London: Springer.
[59]. Rahimi, M. and Rausand, M., *Technology qualification integrated with product development.* International Journal of Performability Engineering 2015. **01**: p. 03-14.
[60]. Zio, E., *Reliability engineering: Old problems and new challenges.* Reliability Engineering & System Safety, 2009. **94**(2): p. 125-141.
[61]. Johansson, C., *On system safety and reliability methods in early design phases, PhD thesis*. 2013, Department of Management and Engineering, Linköping University, Linköping, Sweden.
[62]. MIL-HDBK-217F, *Reliability prediction of electronic equipment*. 1991, Washington, DC: US Department of Defense.
[63]. Prosvirnova, T., *AltaRica 3.0: a Model-Based approach for Safety Analyses.* 2014, Computational Engineering, Finance, and Science [cs.CE] Ecole Polytechnique.
[64]. Rausand, M., *Reliability of Safety-Critical Systems: Theory and Applications*. 2014, Hoboken, NJ: Wiley.
[65]. Parry, G.W., *The characterization of uncertainty in Probabilistic Risk Assessments of complex systems.* Reliability Engineering and System Safety, 1996. **54**: p. 119-126.
[66]. Mosleh, A., Smidts, C., Lui, C. and Siu, N., *Model Uncertainty: Its Characterization and Quantification*. 1995, Maryland: Center for Reliability Engineering, University of Maryland.

[67]. Jin, H., Lundteigen, M.A. and Rausand, M., *Uncertainty assessment of reliability estimates for safety-instrumented systems.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2012. **226**: p. 646-655.
[68]. Zio, E. and Aven, T., *Model Output Uncertainty in Risk Assessment.* International Journal of Performability Engineering, 2013. **29**: p. 475-486.
[69]. Abrahamsson, M., *Uncertainty in quantitative risk analysis - characterisation and methods of treatment*. 2002: PhD thesis.
[70]. NUREG-1855, *Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making*. 2009: Nuclear Regulatory Commision
[71]. NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Guideline*. 2002, Washington, DC: NASA Office of Safetyand Mission Assurance.
[72]. Thunnissen, D.P., *Propagating and mitigating uncertainty in the design of complex multidisciplinary systems*. 2005, PhD thesis: California Institute of Technology.
[73]. Yin, L., Smith, M.A.J. and Trivedi, K.S. *Uncertainty analysis in reliability modeling*. in *Reliability and Maintainability Symposium, Proceedings. Annual*. 2001. IEEE.
[74]. Mechri, W., Simon, C. and Othman, K.B., *Uncertainty analysis of common cause failure in safety instrumented systems.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2011. **225**(4): p. 450=460.
[75]. Bjerga, T., Aven, T. and Zio, E., *An illustration of the use of an approach for treating model uncertainties in risk assessment.* Reliability Engineering & System Safety, 2014. **125**: p. 46-53.
[76]. Droguett, E. and Mosleh, A., *Bayesian Methodology for Model Uncertainty Using Model Performance Data.* Risk Analysis, 2008. **28**(5): p. 1457–1476.
[77]. Lundteigen, M.A. and Rausand, M., *The architectural constraints are meant to compensate for the uncertainty in the PFD estimate.* . Reliability Engineering & System Safety, 2008. **94**: p. 520-525.
[78]. Flage, R., Aven, T. and Zio, E., *Alternative representations of uncertainty in system reliability and risk analysis-review and discussion*, in *European safety and reliability conference (ESREL)*. 2009: Valencia, SPAIN. p. 22-25.
[79]. Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety*. 2011: MIT Press.
[80]. Leveson, N. and Thomas, J., *STPA handbook* 2018: MIT.
[81]. OREDA, *Offshore and Onshore Reliability Data, 6th edition*. 2015.
[82]. Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A. and Bérenguer, C., *Failure rate evaluation with influencing factors.* Journal of Loss Prevention in the Process Industries, 2010. **23**: p. 187-193.
[83]. Rahimi, M. and Rausand, M., *Prediction of failure rates for new subsea systems: A practical approach and an illustrative example.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability August 2013. **227**: p. 629-640.
[84]. ISO/TR12489, *Petroleum, petrochemical and natural gas industries -- Reliability modelling and calculation of safety systems*. 2013, Geneva: International Electrotechnical Commission.

[85]. Zhang, J., Haskins, C., Liu, Y. and Lundteigen, M.A., *A systems engineering based approach for framing reliability, availability and maintainability- A case study for subsea design.* Systems Engineering, 2018. **21**(6): p. 576-592.
[86]. INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 4.0*, ed. G.J.R. D. D. Walden, K. J. Forsberg, K. D. Hamelin, T. M. Shortell. 2015, San Diego, CA: International Council on Systems Engienering: John Wiley and Sons.
[87]. Bahill, A.T. and Gissing, B., *Re-evaluating systems engineering concepts using systems thinking.* Trans. Sys. Man Cyber Part C, 1998. **28**(4): p. 516-527.
[88]. NASA, *NASA Systems Engineering Handbook*. 2007, Washington, D.C.
[89]. Asbjørnsen, O., *Systems engineering principles and practices*. 1992, Maryland, USA: Skarpodd.
[90]. Blanchard, B.S. and Fabrycky, W.J., *Systems engineering and analysis*. 1998, Upper Saddle River, NJ, USA: Prentice-Hall.
[91]. Haskins, C., *Systems engineering analyzed, synthesized, and applied to sustainable industrial park development*. 2008, Tapir Akademisk Forlag 2008:175 (ISBN 978-82-471-1028-7) 141 pages. 141.
[92]. IEEE-STD-1220, *IEEE Standard for Application and Management of the Systems Engineering Process -Description*. 1998
[93]. MIL-STD-499, *Military standard: system engineering management* 1969.
[94]. Haskins, C., *A Systems EngineeringFramework forEco-Industrial Park Formation.* Systems Engineering, 2007. **10**(1): p. 83-97.
[95]. Long, D. and Scott, Z., *A Primer For Model-Based Systems Engineering*. 2012, Blacksburg, VA: Vitech Corporation.
[96]. Dahl, H.J., *Information modelling and systems re-engineering: An efficient approach to assessubg complex current Norwegian natural gas transport operation*, in *Proceedings of Tenth Annual International Symposium on the International Council on Systems Engineering (INCOSE)*. 2000: Minneapolis, US.
[97]. Dahl, H.J., *Norwegian Natural Gas Transportation Systems. Operations in a Liberalized European Gas Market, Ph.D. Thesis*. 2001, Trondheim, Norway: NTNU.
[98]. OMG. *OMG Systems Modeling Language (SysML)* http://www.omg.org/index.htm. 2017 [cited 2017 Nov 17].
[99]. Checkland, P., *Systems Thinking, Systems Practice*. 1999, Chichester, UK: John Wiley.
[100]. Jigar, A.A., Haskins, C. and Lundteigen, M.A. *Availability Allocation Using Systems Engineering Principles*. in *International Conference on Industrial Engineering and Operations Management*. 2016. Kuala Lumpur, Malaysia.
[101]. Garro, A. and Tundis, A., *On the Reliability Analysis of Systems and SoS: The RAMSAS Method and Related Extensions.* IEEE Systems Journal 2015. **9**(1): p. 232-241.
[102]. Shainee, M., Haskins, C., Ellingsen, H. and Leira, B.J., *Designing Offshore Fish Cages Using Systems Engineering Principles.* Systems Engineering, 2012. **15**(4): p. 396-406.
[103]. Ramírez, P.A.P., Utne, I.B. and Haskins, C., *Application of systems engineering to integrate ageing management into maintenance management of oil and gas facilities.* Systems Engineering, 2013. **16**(3): p. 329-345.

[104]. Barnard, R.W.A. *What Is Wrong with Reliability Engineering?* in *Proceedings of the 18th Annual INCOSE International Symposium*. 2008. Utrecht, the Netherlands: International Council on Systems Engineering.
[105]. Friedenthal, S., Moore, A. and Steiner, R., *A Practical Guide to SysML (Third Edition)*. 2015, Boston: Morgan Kaufmann.
[106]. Rausand, M. and Høyland, A., *System Reliability Theory, Models, Statistical Methods, and Applications*. second edition ed. Hoboken, NJ. 2004: John Wiley & Sons, Inc. 419-464.
[107]. Eshuis, R. and Wieringa, R., *Comparing Petri Net and Activity Diagram Variants for Workflow Modelling: A Quest for Reactive Petri Nets.* Petri Net Technology for Communication-Based Systems. LNCS, 2003. **2472**: p. 321-351.
[108]. Yang, N., Yu, H., Sun, H. and Qian, Z. *Mapping UML Activity Diagrams to Analyzable Petri Net Models*. in *2010 10th International Conference on Quality Software*. 2010.
[109]. Andrade, E., Maciel, P., Callou, G. and Nogueira, B. *A Methodology for Mapping SysML Activity Diagram to Time Petri Net for Requirement Validation of Embedded Real-Time Systems with Energy Constraints*. in *2009 Third International Conference on Digital Society*. 2009.
[110]. Eppinger, S.D. and Browning, T.R., *Design Structure Matrix Methods and Applications*. 2012, Cambridge: MIT Press.
[111]. Daniels, J., Werner, P.W. and Bahill, A.T., *Quantitative methods for tradeoff analyses.* Systems Engineering, 2001. **4**(3): p. 190-212.
[112]. Issad, M., Kloul, L. and Rauzy, A., *A scenario-based FMEA method and its evaluation in a railway context*, in *Reliability and Maintainability Symposium (RAMS)*. 2017, IEEE.
[113]. IEC 60300-3-10, *Dependability management-Part 3-10: Application guide Maintainability* 2001.
[114]. Equinor, *Design of a subsea fiscal oil export metering system*, in *NSFMW 2015*. 2015: Tønsberg, Norway.
[115]. Signoret, J.-P., Dutuit, Y., Cacheux, P.-J., Folleau, C., Collas, S. and Thomas, P., *Make your Petri nets understandable: Reliability block diagrams driven Petri nets.* Reliability Engineering & System Safety, 2013. **113**: p. 61-75.
[116]. Signoret, J.-P., *Dependability & Safety Modeling and calculation: Petri Nets*, in *In Proceeding of the 2nd IFAC Workshop on Dependable Control of Descrete Systems*. 2009: Bari, Italy.
[117]. GRIF, *Graphical Interface for reliability Forecasting*. 2016, France: SATODEV.
[118]. AGA-Report No. 9, *Measurement of Gas by Multipath Ultrasonic Meters*. 1998: 1515 Wilson Boulevard, Arlington, VA 22209.
[119]. NORSOK I-106, *Fiscal metering systems for hydrocarbon liquid and gas,*. 2014, Norway: Norsk Sokkels Konkuranseposisjon.
[120]. Kim, H., Lundteigen, M.A., Hafver, A., Pedersen, F. and Skofteland, G., *Application of Systems-Theoretic Process Analysis to isolation of subsea wells: opportunities and challenges of applying STPA to subsea operation*, in *Offshore Technology Conference*. 2018: Houston, Texas, USA.
[121]. Zhang, J., Kim, H., Liu, Y. and Lundteigen, M.A., *Combining System-Theoretic Process Analysis and availability assessment: a subsea case study.* Submitted to Journal of Risk and Reliability 2018.
[122]. Leveson, N. and Thomas, J., *STPA primer version 1*. 2013.
[123]. Rausand, M., *Risk Assessment: Theory, Methods, and Applications*. 2011.

[124]. IEC 61882, *Hazard and operability studies (HAZOP studies)– Application guide*. 2001, International Electrotechnical Commission: Geneva.
[125]. ISO14224, *Petroleum, petrochemical and natural gas industries -- Collection and exchange of reliability and maintenance data for equipment*. 2006: International Organization for Standardization.
[126]. Hauge, S., Lundteigen, M.A., Hokstad, P. and Håbrekke, S., *Reliability pediction method for safety instrumented systems – PDS method handbook. SINTEF report A13503*. 2010, Trondheim, Norway: SINTEF Safety Research.
[127]. IEC 62340, *Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failures.* 2007.
[128]. Hauge, S., Hokstad, P., Håbrekke, S. and Lundteigen, M.A., *Common cause failures in safety-instrumented systems: Using field experience from the petroleum industry.* Reliability Engineering & System Safety, 2016. **151**: p. 34-45.
[129]. Lundteigen, M.A. and Rausand, M., *Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing.* Journal of Loss Prevention in the Process Industries, 2007. **20**: p. 218-229.
[130]. DNV-RP-D102, *Failure Mode and Effect Analysis (FMEA) of Redundant Systems*. 2012, Høvik, Norway: DNV.
[131]. Childs, J.A. and Mosleh, A., *A modified FMEA tool for use in identifying and addressing common cause failure risks in industry*, in *Reliability and Maintainability Symposium*. 1999, IEEE: Washington, DC. p. 19-24.
[132]. Giardina, M. and Morale, M., *Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology.* Journal of Loss Prevention in the Process Industries, 2015. **35**: p. 35-45.
[133]. Seligmann, B.J., Németh, E., Hangos, K.M. and Cameron, I.T., *A blended hazard identification methodology to support process diagnosis.* Journal of Loss Prevention in the Process Industries, 2012. **25**(4): p. 746-759.
[134]. Rasmussen, J., *Risk management in a dynamic society: a modelling problem.* Safety Science, 1997. **27**(2): p. 183-213.
[135]. Hollnagel, E., *FRAM:The functional resonance analysis method:modelling complex socio-technical systems*. 2012 Farnham: Ashgate Publishing Ltd.
[136]. Abdulkhaleq, A., Lammering, D., Wagner, S., Röder, J., Balbierer, N., Ramsauer, L., Raste, T. and Boehmert, H., *A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles.* Procedia Engineering, 2017. **179**(Supplement C): p. 41-51.
[137]. Faiella, G., Parand, A., Franklin, B.D., Chana, P., Cesarelli, M., Stanton, N.A. and Sevdalis, N., *Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach.* Reliability Engineering & System Safety, 2018. **169**(Supplement C): p. 117-126.
[138]. Nakao, H., Katahira, M., Miyamoto, Y. and Leveson, N. *safety guide design of crew return vehicle in concept design phase using STAMP/STPA*. in *Proceeding of the 5th IAASS Conference* 2011. Citeseer.
[139]. Kim, H., Lundteigen, M.A., Hafver, A., Pedersen, F., Skofteland, G., Holden, C. and Ohrem, S.J., *Application of Systems-Theoretic Process Analysis to a Subsea Gas Compression System*, in *ESREL* 2018: Trondheim, Norway.

[140]. Young, W. and Leveson, N., *Systems thinking for safety and security*, in *Proceedings of the 29th Annual Computer Security Applications Conference*. 2013, ACM: New Orleans, Louisiana, USA. p. 1-8.
[141]. Friedberg, I., McLaughlin, K., Smith, P., Laverty, D. and Sezer, S., *STPA-SafeSec: Safety and security analysis for cyber-physical systems.* Journal of Information Security and Applications, 2017. **34**: p. 183-196.
[142]. Rodríguez, M. and Díaz, I., *A systematic and integral hazards analysis technique applied to the process industry.* Journal of Loss Prevention in the Process Industries, 2016. **43**: p. 721-729.
[143]. Wróbel, K., Montewka, J. and Kujala, P., *System-theoretic approach to safety of remotely-controlled merchant vessel.* Ocean Engineering, 2018. **152**: p. 334-345.
[144]. Mahajan, H.S., Bradley, T. and Pasricha, S., *Application of systems theoretic process analysis to a lane keeping assist system.* Reliability Engineering & System Safety, 2017. **167**: p. 177-183.
[145]. Sulaman, S.M., Beer, A., Felderer, M. and Höst, M., *Comparison of the FMEA and STPA safety analysis methods–a case study.* Software Quality Journal, 2017.
[146]. Rokseth, B., Utne, I.B. and Vinnem, J.E., *Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis.* Reliability Engineering & System Safety, 2018. **169**(Supplement C): p. 18-31.
[147]. Hafver, A., Eldevik, S., Jakopanec, I., Drugan, O.V., Pedersen, F., Flage, R. and Aven, T., *Risk-based versus control-based safety philosophy in the context of complex systems*. 2017. 38-38.
[148]. Thomas, J., *Extending and Automating STPA for Requirements Generation and Analysis, Ph.D. Dissertation*. 2013: MIT.
[149]. Balbo, G., *Introduction to Generalized Stochastic Petri Nets*, in *Formal Methods for Performance Evaluation: SFM*, M. Bernardo and J. Hillston, Editors. 2007, Springer Berlin, Heidelberg. p. 83-131.
[150]. Marsan, M.A., Balbo, G., Chiola, G., Conte, G., Donatelli, S. and Franceschinis, G., *An introduction to generalized stochastic Petri nets.* Microelectronics Reliability, 1991. **31**(4): p. 699-725.
[151]. Rokseth, B., Utne, I.B. and Vinnem, J.E., *A systems approach to risk analysis of maritime operations.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2016. **231**(1): p. 53-68.
[152]. Berner, C. and Flage, R., *Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions.* Reliability Engineering & System Safety, 2016. **151**: p. 46-59.
[153]. Zhang, J., Liu, Y., Lundteigen, M.A. and Bouillaut, L., *Using Bayesian Networks to quantify the reliability of a subsea system in the early design* in *ESREL*. 2016: Glasgow, UK.
[154]. exida, *Safety Equipment Reliability Handbook - 4th Edition*. 2015.
[155]. SINTEF, *Reliability Data for Safety Instrumented Systems - PDS Data Handbook, S.Hauge, T.Onshus (Authors)*. 2010: SINTEF.
[156]. Lindqvist, B. and Tjelmeland, H., *An exponential regression model for censored failure data: Estimation and graphical model checking*, in *10th annual symposium of the Society of Reliability Engineers*. 1989: Stavanger, Norway.
[157]. Kumar, A., *Reliability Assessment of Subsea Production Valves*. 2015, Department of Production and Quality Engineering, Norwegian University of Science and Technology.

[158]. Vinnem, J.E., Seljelid, J., Haugen, S., Sklet, S. and Aven, T., *Generalized methodology for operational risk analysis of offshore installations.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2008. **223**(1): p. 87-97.
[159]. Brissaud, F., Barros, A., Bérenguer, C. and Charpentier, D., *Reliability analysis for new technology-based transmitters.* Reliability Engineering & System Safety, 2011. **96**: p. 299-313.
[160]. Cai, B., Liu, Y., Fan, Q., Zhang, Y., Yu, S., Liu, Z. and Dong, X., *Performance evaluation of subsea BOP control systems using dynamic Bayesian networks with imperfect repair and preventive maintenance.* Engineering Applications of Artificial Intelligence, 2013. **26**: p. 2661-2672.
[161]. Jones, B., Jenkinson, I., Yang, Z. and Wang, J., *The use of Bayesian network modelling for maintenance planning in a manufacturing industry.* Reliability Engineering & System Safety, 2010. **95**: p. 267-277.
[162]. Zitrou, A., *Exploring a Bayesian approach for structural modelling of common cause failures (Ph.D thesis)*. 2006: University of Strathclyde. Department of Management Science.
[163]. Jensen, F.V., *An introduction to Bayesian Networks*. 1996, NJ, USA: Springer.
[164]. Khakzada, N., Khana, F. and Amyotte, P., *Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network.* Process Safety and Environmental Protection, 2013. **91**: p. 46-53.
[165]. Ascher, H. and Feingold, H., *Repairable systems reliability: modeling, inference, misconceptions and their causes*. 1984: Marcel Dekker.
[166]. Vatn, J., *Risk_OMT-Hybrid approach, Course PK8200-Risk Influence Modelling and Risk Indicators*. 2013, Norway: NTNU.
[167]. Bobbio, A., Portinale, L., Minichino, M. and Ciancamerla, E., *Improving the analysis of dependable systems by mapping fault trees into bayesian networks.* Reliability Engineering and System Safety, 2001. **71**: p. 249–260.
[168]. HUGIN, *software version 8.2* http://www.hugin.com. 2015.
[169]. Bayes Net Toolbox for Matlab (Written by Kevin Murphy). https://www.cs.utah.edu/~tch/notes/matlab/bnt/docs/bnt_pre_sf.html. 2003.
[170]. IEC61508, *Functional safety of electrical/electronic/programmable electronic safety related systems. Part 1-7*. 2010, Geneva: International Electrotechnical Commission.
[171]. Geng, Z., Yang, F., Chen, X. and Wu, N., *Gaussian process based modeling and experimental design for sensor calibration in drifting environments.* Sensors and Actuators B: Chemical, 2015. **216**: p. 321-331.
[172]. Moranda, P.B., *Prediction of Software Reliability During Debugging*. 1975.
[173]. Innal, F., *Contribution to modelling safety instrumented systems and to assessing their performance: Critical analysis of IEC 61508 standard, PhD Thesis*. 2008, Bordeaux: University of Bordeaux
[174]. Oliveira, L.F., *Evaluating the PFD of instrumented safety systems with partial stroke testing*. Vol. 2. 2008. 1090-1097.
[175]. Vaurio, J.K., *Unavailability equations for k-out-of-n systems.* Reliability Engineering & System Safety, 2011. **96**(2): p. 350-352.
[176]. Jahanian, H., *Generalizing PFD formulas of IEC 61508 for KooN configurations.* ISA Transactions, 2015. **55**: p. 168-174.
[177]. IEC 61025, *Fault tree analysis (FTA)*. 2006.
[178]. IEC 61078, *Reliability block diagrams*. 2016.

[179]. Li, R., Liu, X. and Huang, N., *Availability Allocation of Networked Systems Using Markov Model and Heuristics Algorithm.* Mathematical Problems in Engineering, 2014. **2014**: p. 9.
[180]. IEC 61165, *Application of Markov techniques*. 2006.
[181]. Balbo, G., *Introduction to Generalized Stochastic Petri Nets*, in *Formal Methods for Performance Evaluation: 7th International School on Formal Methods for the Design of Computer, Communication, and Software Systems, SFM 2007, Bertinoro, Italy, May 28-June 2, 2007, Advanced Lectures*, M. Bernardo and J. Hillston, Editors. 2007, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 83-131.
[182]. Felgner, F. and Frey, G., *Multi-Phase Markov Models for Functional Safety Prediction: Efficient simulation of Markov models used for safety engineering and the online integration of individual systems' diagnostic and maintenance history*, in *Dependable Control of Discrete Systems (DCDS) 3rd International Workshop on*. 2011.
[183]. Brameret, P.-A., Rauzy, A. and Roussel, J.-M., *Automated generation of partial Markov chain from high level descriptions.* Reliability Engineering & System Safety, 2015. **139**: p. 179-187.
[184]. Durga Rao, K., Gopika, V., Sanyasi Rao, V.V.S., Kushwaha, H.S., Verma, A.K. and Srividya, A., *Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment.* Reliability Engineering & System Safety, 2009. **94**: p. 872-883.
[185]. Xing, L., Shresthac, A. and Dai, Y., *Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures.* Reliability Engineering & System Safety, 2011. **96**(10): p. 1375-1385.
[186]. Batteux, M., Prosvirnova, T. and Rauzy, A., *System Structure Modeling Language (S2ML).* 2015.
[187]. Rauzy, A., *Guarded transition systems: A new states/events formalism for reliability studies.* Proceedings of the Institution of Mechanical Engineers. Part O, Journal of risk and reliability, 2008. **222**(4).
[188]. Batteux, M., Prosvirnova, T. and Rauzy, A., *System Structure Modeling Language (S2ML)*. 2015.
[189]. Prosvirnova, T. and Rauzy, A., *AltaRica 3.0 project: compile Guarded Transition Systems into Fault Trees*, in *ESREL2013*. 2013.
[190]. Lipaczewski, M., Ortmeier, F., Prosvirnova, T., Rauzy, A. and Struck, S., *Comparison of modeling formalisms for Safety Analyses: SAML and AltaRica.* Reliability Engineering & System Safety, 2015. **140**: p. 191-199.
[191]. Kloul, L., Prosvirnova, T. and Rauzy, A., *Modeling systems with mobile components: a comparison between AltaRica and PEPA nets.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2013. **227**(6).
[192]. Martorell, P., Martón, I., Sánchez, A.I. and Martorell, S., *Unavailability model for demand-caused failures of safety components addressing degradation by demand-induced stress, maintenance effectiveness and test efficiency.* Reliability Engineering & System Safety, 2017. **168**(Supplement C): p. 18-27.
[193]. Peng, G., *On human errors in maintenance: risk potential and mitigation (Master thesis)*. 2014: University of Stavanger.
[194]. Hafver, A., Lindberg, D., Eldevik, S. and Pedersen, F., *Imperfect versus incomplete testing: Implications for safety*. 2016. 1520-1525.

[195]. Maros and Taro. https://www.dnvgl.com/services/ram-analysis-software-for-upstream-oil-and-gas-maros-1152. 2018 [cited 2018.
[196]. IEC 60300 3-4, *Dependability management - Guide to the specification of dependability requirements*. 2007.
[197]. MIL-HDBK-338B, *Electronic Reliability Design Handbook*. 1998: US Department of Defense.
[198]. Alven, W., *Reliability engineering, prepared by arinc research corporation* 1964, Washington, D.C: Englewood Cliffs, N.J., Prentice-Hall.
[199]. AGREE, *Reliability of military electronic equipment* 1957, Washington, DC.: Office of the Assistant Secretary of Defense Research and Enginnering.
[200]. Mettas, A. *Reliability Allocation and Optimization for Complex Systems*. in *Proceedings of the annual maintainability and reliability symposium*. 2000. Los Angles,California: 216-.
[201]. Yadav, O.P. and Zhuang, X., *A practical reliability allocation method considering modified criticality factors.* Reliability Engineering & System Safety, 2014. **129**: p. 57-65.
[202]. Kuo, W. and Wan, R., *Recent Advances in Optimal Reliability Allocation.* IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 2007. **37**(2): p. 143-156.
[203]. Amari, S.V. and Hegde, V. *New allocation methods for repairable systems*. in *Reliability and Maintainability Symposium*. 2006. Newport Beach, CA: IEEE.
[204]. Jigar, A.A., Lundteigen, M.A. and Liu, Y., *A New Availability Allocation Method*, in *ESREL 2015 Conference* 2015: ETH, Zurich.
[205]. Vintr, Z., Hasilova, K. and Vintr, M., *A mathmatical model for preliminary reliability and maintainability allocation*, in *ESREL2018*. 2018: Trondheim, Norway.
[206]. Kuo, W., *An Annotated Overview of System-Reliability Optimization.* IEEE transactions on reliability 2000. **49**: p. 176-187.
[207]. Boyd, J.A. *Allocation of reliability requirements: a new approach* in *proceedings of reliability and maintainability symposium* 1992. Las Vegas, NE.
[208]. Bracha, V.J., *The methods of reliability engineering.* Machine Design, 1964. **7**: p. 70-76.
[209]. Chang, Y., Chang, K. and Liaw, C., *Innovative reliability allocation using the maximal entropy ordered weighted averaging method.* Computers & Industrial Engineering, 2009. **57**: p. 1274-1281.
[210]. Wang, Y., Yam, R.C.M., Zuo, M.J. and Tse, P., *A comprehensive reliability allocation method for design of CNC lathes.* Reliability Engineering & System Safety, 2001. **72**: p. 247-252.
[211]. MIL-HDBK-470A, *Department of defense handbook- designing and developing maintainable products and systems* 1997.
[212]. Liang, Q., Song, B. and Zhao, M., *Study on the methods of maintainability allocation of under water vehicle.* WRI world congress On computer science and information engineering, 2009: p. 256-261.
[213]. Amari, S.V. and Hegde, V. *New Allocation Methods for Repairable Systems* in *Annual Reliability and Maintainability Symposium*. 2006. Newport Beach, CA.
[214]. Barabady, J. and Kumar, U., *Availability allocation through importance measures.* International Journal of Quality & Reliability Management, 2007. **24**: p. 643-657.

[215]. Sagaspe, L. and Bieber, P. *Constraint-based design and allocation of shared avionics resources*. in *2007 IEEE/AIAA 26th Digital Avionics Systems Conference*. 2007.

APPENDICES

- List of acronyms and abbreviations
- Conference Paper: ESREL 2016
- Conference Paper: RQD 2017
- Journal paper: Systems Engineering 2018
- Journal paper: Journal of Risk and Reliability 2018 (revised manuscript under review)

List of acronyms and abbreviations

AGREE	Advisory Group on Reliability of Electronic Equipment
ARINC	Aeronautical Radio Inc
BN	Bayesian Network
BORA	Barrier and Operational Risk Analysis
CAD	Computer Aided Design
CAPEX	Capital Expenditure
CCF	Common Cause Failure
CPT	Conditional Probability Tables
CVM	Choke Valve Module
DAG	Directed Acyclic Graph
DSM	Design Structure Matric
EPU	Electrical Power Unit
ESP	Electrical Submersible Pump
FEM	Finite Element Method
FFBD	Function Flow Block Diagram
FMECA	Failure mode, Effects and Criticality Analysis
FRAM	Functional Resonance Analysis Method
FSA	Finite State Automata
FTA	Fault Tree Analysis
GTS	Guarded Transition Systems
HAZOP	Hazard and Operability Study
HIPPS	High Integrity Pressure Protection System
HPU	Hydraulic Power Unit
IEV	International Electrotechnical Vocabulary
IMR	Inspection, Maintenance and Repair
INCOSE	International Council on Systems Engineering

KooN	K out of N
MBSE	Model-Based Systems Engineering
MC	Monte Carlo
MCS	Master Control Station
MPM	Multiphase Pump Module
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAT	Normal Accident Theory
NOK	Norwegian Kroner
NHPP	Nonhomogeneous Poisson Process
O&G	Oil and Gas
OPEX	Operational Expenditure
OREDA	Offshore and Onshore Reliability Data
PCS	Process Control System
PSA	Petroleum Safety Authority
PSD	Process Shutdown system
PT	Pressure Transmitters
QFD	Quality Function Deployment
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RHF	Random Hardware Failures
RIF	Reliability influencing factor
ROV	Remotely Operated Vehicle
SAT	Site Acceptance Testing
SADT	Structure Analysis and Design Technique
SC	System-level Constraints
SCM	Subsea Control Module

SCU	Subsea Control Unit
SDU	Subsea Distribution Uunit
SE	Systems Engineering
SEM	Subsea Electronic Module
SF	Systematic Faults
SGB	Subsea Gate Box
SH	System-level Hazard
SoS	System of Systems
SPM	Separation Module
SPN	Stochastic Petri-Nets
STAMP	Systems Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
SUBPRO	Subsea Production and Processing
SWIFT	Structured What-If checklist
SysML	System Modelling Language
TQP	Technology Qualification Program
TT	Temperature Transmitters
TRL	Technology Readiness Level
UCA	Unsafe Control Action
UML	Unified Modelling Language
USM	Ultrasonic Flow Meter
XOV	Crossover Valve
ZA	Zonal Analysis

Using Bayesian networks to quantify the reliability of a subsea system in the early design

Zhang J, Liu Y, Lundteigen MA, Laurent Bouillaut. Using Bayesian networks to quantify the reliability of a subsea system in the early design. *Presented at ESREL 2016 September, Glasgow, UK*

Using Bayesian Networks to quantify the reliability of a subsea system in the early design

J.Zhang, Y. Liu & M.A. Lundteigen
Department of Production and Quality Engineering
Norwegian University of Science and Technology, Trondheim, Norway
L.Bouillaut
University Paris-Est, IFSTTAR, GRETTIA, F-93166 Noisy-le-Grand, France

ABSTRACT: Quantification of the reliability of systems is an essential task when evaluating new technologies, since a lack of adequate reliability performance will violate the intended gain of the innovation. Several models for reliability assessment have been proposed in literature. However, they are often criticized for not being very useful in early evaluations of new design concepts, as they may not be able to include new operating aspects in the models, such as new ways of operating and new environmental exposures. Bayesian formalism, as a probabilistic modeling approach, is experiencing a growing success due to its flexibility in modelling various system features. This paper reviews the valuable features offered by Bayesian formalism, and explores the possible advantages of using Bayesian Networks for reliability assessment in the early design phase of subsea systems. The applicability of adapting Bayesian formalism for this purpose has been demonstrated using a high integrity pressure protection system installed on the seabed to protect a hydrocarbon pipeline against overpressures.

1 INTRODUCTION

Reliability is one of the key performance measures of technical systems used to demonstrate the ability of the system to carry out the desired function over time (Rausand & Høyland, 2004). The reliability of a structured system can be evaluated by using the suitable modelling approach to show how the potential events (e.g. component failure, maintenance and testing) can influence the system failure. The quantification of reliability can form as a basis for decision-making concerning different stages of the system development process (i.e. design, construction and operation and maintenance) (Rausand, 2014).

An overview of modelling approaches available to quantify reliability may be found in literature (Rausand, 2014; Rausand & Høyland, 2004). However, none of the modelling approaches can fit for all types of systems, especially when the operational philosophies of the selected system are complex and the associated effect remains dormant to analysts at the early stage.

Reliability influencing factor (RIF) can represent conditions that have impact on the loss of system performance, e.g. test and maintenance strategies, human and organizational factors (HOFs), environmental factors and so on (Lundteigen & Rausand, 2010). All relevant RIFs can in principle be included in the reliability model, but the precision in the calculated result may not necessarily be very high if the data is uncertain or not available, or invalid assumptions are made in the model(s). In practice, it seems more feasible to build a model that accounts for the most important factors instead of considering all factors of relevance with low-quality data input. This is especially the case when assessing reliability of a new (unproven) technology or system in the early stage of the design, where the details of the system have not yet been settled and few data are available.

The subsea oil and gas industry is one example of an industrial sector where innovations are needed to reduce costs and to meet stricter safety requirements. The industry is conducting a high number of reliability assessments, but experience indicate that they are carried out too late to have an effect on early design selections and decisions. To support the need to use reliability assessments more actively in the early verification of new subsea design concepts, it is necessary to develop reliability modelling approaches that can capture the most important characteristics of systems performance in its (new) operating environment,

and the most important effects of uncertainty associated with these.

The objective of this paper is to adapt Bayesian formalism in reliability assessment in the early design phase, and to demonstrate how it can be applied for an oil and gas related safety system to be installed subsea. The outline of the paper is shown as follows: Section 2 introduces the basic concept of modelling approach in the reliability assessment, and points out challenges of developing feasible reliability model in light of subsea systems. Section 3 briefly reviews basic features of Bayesain Networks and explore the possible use in the reliability assessment for subsea systems. The applicability of proposed approach is illustrated by an example of subsea high integrity pressure protection system in Section 4. In the end, the discussion and conclusion are presented in Section 5.

2 CHALLENGES IN MODELLING SUBSEA RELIABILITY

The term *model* is always an abstraction of the reality of a real system (Long, 2012). A model can be used to qualitatively express functions in a system and with surroundings, or quantify a suitable measure of a specific system performance. The focus of this paper is only placed on the quantitative model to estimate the reliability of a structured system, which is built up on a basis of a logic model to study how the system fails, within input parameters (i.e. the failure data for selected failures). An overview of models used for reliability assessment can be found in many textbooks and standards. For safety-instrumented systems (SIS) that are required to perform their intended function upon demand, the useful reference are part 6 of IEC61508 (2010) and ISO/TR12489 (2013), and the limitation and the application of these models can be found in a number of literatures (Innal, 2008; Johansson, 2013; Rausand & Høyland, 2004). Most of current models for reliability or availability assessment (if downtime associated with e.g. repairs of system are included) focus on describing how the state of system changes in certain of events, such as failure, testing, repair and so forth. The probabilistic distribution is used to describe the occurrence of the event, such as failures of component which by definition we don't know when will it happen.

The term *failure* can be interpreted differently according to performance characteristics of systems. The success/failure of system performance is relatively easy to define within yes/no decision boundary, such as the safety function. However, developing the reliability model for the system with variable performance characteristic, requires several attempts to clearly determine unacceptable levels (or failure) of system performance (MIL-HDBK-338B, 1998). It is especially the case for subsea production and processing system where the difficulty of mitigating failures subsea is much higher than topside due to limited and costly access. This situation calls for alternative ways or 'soft means' to maintain reliability performance above the limits of acceptable performance over time, and the corresponding reliability model should therefore encounter for degraded mode of operation. However, some static models such as Fault Tree Analysis (FTA) and Reliability Block Diagram (RBD) will not be able (at least in an easy way) to model the degraded operation. Moreover, basic events in the standard FTA are statistically independent, meaning that dependencies between failures are impossible to address in standard fault tree (Bobbio, Portinale, Minichino, & Ciancamerla, 2001).

Many systems installed on the seabed also involve dynamic system behaviors because of the complex way of operating. Some models such as Markov analysis (MA) and Petri Nets (PN) are able to give a realistic picture about dynamic features of systems in case of certain events (Rausand, 2014). However, the model based on Markov property are often criticized for the exponentially increasing size of model when modelling the system with a high level of complexity. PN may be recommended when there is a necessity to consider operational aspects such as maintenance, but it is hard to develop PN and even more hard to update the PN model when more details of system is given.

The selection of reliability model does not only depend on the type of systems, but also the stage of its development. As of today, the oil and gas industry is frequently using qualitative models (e.g. FTA and RBD are used as structure analysis) in the early design phase, and the more advanced modelling approaches are often pursued in the later stage and they are used for verification and not for design evaluation as the possibilities to influence the design is limited at this stage (equipment already ordered, decisions about technical solution taken). The use of quantitative models in early phase may also be criticized due to a lack of suitable data and details/information of system operation (Johansson, 2013). Many of the future developments in subsea require adaption of new technology and new ways of operating, however, may involve uncertainty in many aspects. For reliability assessment, the uncertainty can be categorized as *model uncertainty*, *data/parameter uncertainty and completeness uncertainty*. As the limited knowledge about the new system becoming one particular issue for early design, the completeness uncertainty is of greatest importance, followed by model and data uncertainty (Jin, Lundteigen, & Rausand, 2012). The uncertainty should be addressed in the early evaluation to avoid the situation that too conservative design is selected to compensate for the uncertainty caused by unfamiliar operating conditions and a lack of historic performance in the beginning of development process.

Therefore, models used as basis for reliability assessment of subsea systems, also for use in the early design phase, should therefore address foreseeable

situations where operation in degraded mode is required, the complex operational phenomenon, and incorporate the result of simulation (in an early design phase) as the reliability data under uncertainty. However, the classical reliability modelling approaches do not suffice for this purpose. This paper will discuss valuable features offered by Bayesian Networks, and explore the possible use for reliability assessment in the early design phase of subsea systems.

3 BAYESIAN NETWORKS

3.1 *Basic features of Bayesian Networks*

Bayesian Networks (BN), are used in many engineering or science disciplines since their emergence, such as artificial intelligence development and the decision-making strategy. This formalism has been recently introduced in field of reliability, availability and maintainability (RAM) analysis and experienced a growing success because of its flexibility in modelling various system features. This modelling approach, based on the Bayesian theory, can be used as a better alternative to FTA as the restrictive assumptions of FTA can be removed and dependencies between failures are incorporated in BN model (Bobbio et al., 2001). The BN model can also build up the cause-effect relationships between the multi-state variables, e.g. failure rate of a system and associated contributing factors (Jones, Jenkinson, Yang, & Wang, 2010). Many other applications of the BN formalism can also be found in the past decade literature, proving its ability to model reliability and maintenance strategies, see (Cai et al., 2013; Cai et al., 2012).

BN can be expressed as a graphical representation which consists of Directed Acyclic Graph (DAG) formed by variables together with the directed edges, and Conditional Probability Tables (CPT) assigned the conditional dependencies between variables (Jensen, 1996). When a link connects a node A to another node B, A is a *parent* of B and the variables that the two nodes denote are conditionally dependent. If the node A has not any parent, it is called as a *root node* and its *prior probability* should be specified in the CPT. The joint probability distribution of a set of variables $[X_1,X_2 \ldots X_n]$ is given as follows (Jensen, 1996), where $Pa\ (X_i)$ refers to the parent of X_i:

$$Pr[X_1,X_2 \ldots X_n] = \prod_{i=1}^{n} Pr[X_i|Pa\ (X_i)] \quad (1)$$

One of the most unique ability of BN is to compute the *posterior probability* of any nodes when the observation of a set of variable E, called as *evidence* is given. The prior probability can therefore be updated by taking advantages of *Bayes' theorem* (Khakzada, Khana, & Amyotte, 2013):

$$Pr(U|E)Pr(E) = Pr(E|U)Pr(U) \quad (2)$$

3.2 *Bayesian Networks in reliability assessment*

The valuable features offered by using BN model have already been discussed by some researchers, see e.g. (Bobbio et al., 2001; Jones et al., 2010; Khakzada et al., 2013; Rausand & Høyland, 2004). Some key factors driving the implementation of Bayesian formalism in reliability assessment can be summerized by comparing to the most widespread modelling approach in reliabiltity assement, i.e. FTA.

The states of variables being modelled in BN do not have to be binary as for FTA, so that the multi-states variables can be easily accommodated. The standard FTA has to connect the variables/events through a specified logic gates (i.e. AND-gate and OR-gate). This issue can be solved by using some advanced FTA tooling (e.g. dynamic fault tree) by including some other type of gates, see (Durga Rao et al., 2009). While for BN models, it is possible to involve probabilistic gates, which are able to develop the complicated cause-effect relationship between variables, e.g. the failure and failure causes, the failure causes and the contributing factors.

The statistical dependencies between variables can be easily accommodated and visualized in the BN models by modifying the CPT and adding the causal arcs to connect variables. For example, in a fault tree common because failures (CCFs) and individual failures are assumed be necessarily independent, but such assumption is not needed in a BN model. In FTA, a CCF can be treated explicitly as the single input to the system failure by adding an OR-gate, or the CCF can be treated implicitly by considering it as a minimal cut set. In a BN model, a CCF can be modeled by identifying the relationships between failure causes. As shown in Figure 1, where C_i stands for the cause that leads to the failure of component X_j (connected by causal arc) and F stands for state of system consists of component X_j. In the Figure 1 (a), the root variable C_i are uncorrelated so that only C_2 act as the CCF that can lead to the failure of both X_j. In this case, we can modify the Figure 1 (a) to Figure 1 (c), treating the CCF as one direct input to the system failure. Figure 1 (b), the root node consists of all the correlated causes so that the joint probability for all C_i should be specified in the CPT, which can avoid incorrect inclusion of dependent common causes.

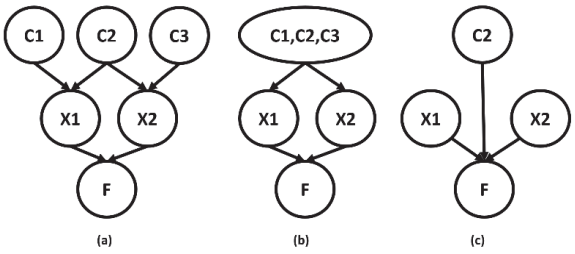


Figure 1. (a) Uncorrelated causes, (b) Correlated cause and (c) Common cause C_2

Besides above, the ability to update estimation according to new information (e.g. failure rate of components or reliability of selected systems) makes BN model an appealing candidate for reliability assessment in the later phase of system development. It can be used to update estimates based on the data derived from the site acceptance testing (SAT). The detailed discussion about updating procedures using influencing algorithm within cumulative collection of occurrence over a certain interval can be found in (Khakzada et al., 2013). The updating technique can also be used in the operational phase, to forecast the change in trends that may suggest a variation in estimated reliability, based on monitoring technical states and process parameters of critical components (e.g. conditional monitoring or even online monitoring). Some similar works have already been done in the domain of risk analysis, see (Vatn, 2013). In this paper, we will study the suitability of using BN in the early design phase.

3.3 *Quantifying reliability of subsea systems with BN*

An interesting possibility is to take advantages of Bayesian formalism to provide an approximate indication of reliability achievement of subsea innovation at the early stage, which (at least) includes the following aspects:

1) Degraded mode of operation
2) Foreseeable operational conditions
3) Flexible inclusion of RIFs

3.3.1 *Degraded mode of operation*

The variable performance characteristics can be expressed as discrete nodes in the BN. As discussed above, the operators of subsea system usually want to continue operation in case of certain type of failures, meaning a reduction in information or performance. Once the acceptable level of performance is clearly determined, subsea components/systems can be in one of the following states: (i) *fully (perfectly) working state*, (ii) *degraded working state* where the components/systems work at the reduced level but above the limit and (iii) *faulty state* where the performance of components/systems is considered unsatisfactory. Even for the safety system that only includes go/no-go performance attributes, the number of states in the variable can be more than two, depending on the level of redundancy. For instance, a two-of-three voted system can have three states expressed as [fully working (3oo3), degarded working (2oo3), faulty (1oo3 or 0oo3)].

3.3.2 *Foreseeable operational conditions*

In subsea applications, known systems or technologies may be exposed to unfamiliar failure causes due to changes of operating environment and novelty itself. The impact of failure causes cannot be fully revealed based on historical data in the early design phase of new subsea application. Using probabilistic gates instead of logic gates can illustrate the relationship between the failure and its causes, and components are allowed to response differently to one particular failure cause. The uncertainty about unknown or unfamiliar relationship between failure causes and failures can therefore be outlined in the calculated result. For reliability assessment in the early design, the effects of foreseeable operational conditions will be unknown or uncertain, but the BN model can allow their inclusion while relying heavily on the other type of information (e.g. expert judgment, the relevance between industrial sectors). Therefore, the best estimates of uncertainty should be taken into account.

3.3.3 *Flexiable inclusion of RIFs*

The failure rate of component is an essential parameter input of reliability model, and it can be correspondingly assigned as the prior probability for the failure of each component in BN model. The estimation of failure rate for new equipment may be on the basis of evaluating relevant RIFs, see e.g. (Brissaud, Charpentier, Fouladirad, Barros, & Bérenguer, 2010; Rahimi & Rausand, 2013). BN may allow a more flexible inclusion of RIFs, in light of following topics for failure rate estimation:

- Selection of RIFs:

The list of RIFs may vary depending on types of systems and their intended application areas. Some generic RIFs can be found in (Brissaud et al., 2010). The RIFs of subsea systems should be collected based on the expert opinions, experience from existing subsea application and recommendations from stakeholders. Normally the RIFs are selected as disjoint as possible since linear relationship are often assumed between RIFs and failure causes (Rahimi & Rausand, 2013). However, the selected RIFs can be disjoint or correlated as dependencies between variables can be easily accomadated in Bayesian formalism.

- Assign values of RIFs:

Some RIFs like temperature are directly related to a measurement (e.g. the measured or foreseen value), but other RIFs cannot be easily measured, such as HOF or maintenance strategies. This paper tacitly assumes that RIFs can be treated as the stochastic variables in BN, meaning that all RIFs can be updated and estimated based on the mutual information (e.g. indicators, failure propagation and historical events).

According to the Bayesian philosophy, a random variable A, with some density function of $f(A)$ that can express what one thinks about the occurring value of A, before any evidence are obtained (Rausand & Høyland, 2004). Therefore, it is possible to account for the effect of uncertainty by allocating suitable probability distribution to the variables, for example, the beta distribution for continuous variables (Vatn, 2013). If one variable A in a binomial distribution is

beta distributed within prior shape parameter α_0 and β_0, the posterior probability of A is still beta-distributed within posterior shape parameter α_0+s and β_0 +n-s, where s denotes the number of n trials that have outcome as outcome X. In this paper, only the discrete nodes are used to represent RIFs for calculation convenience.

- Connecting RIFs to failure causes

The influencing functions between RIFs and their child nodes (i.e. failure causes) can be determinted by building up the cause-effect relationship probabilistically. This is essentially based on expert judgement and system/function analysis. A high degree of uncertainty may therefore dominate the results of the reliability assessment due to biased judgement. One possible solution to overcome this obstacle in the BN model is to introduce different experts as a root node connecting to the failure causes, where the priors of node 'expert' are the weights of each expert. Therefore, failure-derived data can be used to adjust the weights of experts.

4 EXAMPLE

The subsea production and processing system faces a number of challenges in evaluating reliability of subsea units as they are installed in a harsh and unfamiliar working environment. This section demonstratse the applicability of proposed approach by modelling a specific failure phenomena that influence the performance of system installed subsea. This type of system is not new, but we can foresee that new type of equipment is introduced (e.g., for sensors) to enhance reliability. The computation and graphical representation of BN model is done by the software HUGIN (2015).

4.1 *System description*

A high integrity pressure protection system (HIPPS) is normally combined with process shutdown system to protect the downstream equipment from the overpressure. The schematic of HIPPS is illustrated in Figure 2.

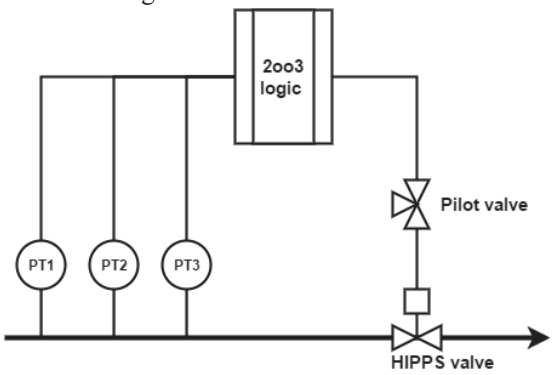


Figure 2. schematic of HIPPS functions

Figure 3. RBD for HIPPS function

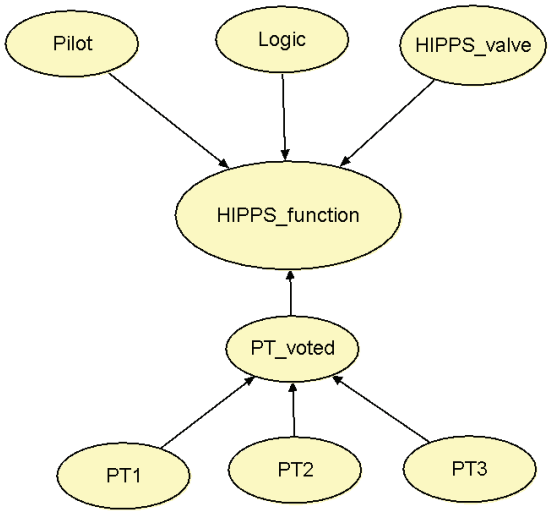


Figure 4. BN model for HIPPS function

The HIPPS is a typical SIS that can be divided into three modules: (i) a two-out-of-three (2oo3) voted pressure transmitter (PT) system as a *sensor* module, (ii) a *logic* module, and (iii) a HIPPS valve that equipped with pilot valve as the *final element* module to stop the flow from upstream to downstream facilities under overpressure situation. The RBD of the HIPPS function is illustrated in Figure 3. The BN model in Figure 4 can be constructed on basis of RBD, where probability of system failure is the prior probability of variable 'HIPPS_function'. The 2oo3 voted system means that the system is able to respond when at least two PTs are functioning. The 2oo3 voted system in RBD model is considered as binary variable, whereas three states are assigned for this variable in BN model according to the discussion in section 3.3.1.

Table 1 lists the associated failure rate and prior probability of each components, based on the data provided in PDS data handbook (SINTEF, 2010). Since the demand rate of HIPPS is lower than once per year, the average probability of failure on demand (PFD_{avg}) is selected as the measure of reliability as suggested by IEC61508 (2010). The PFD_{avg} (priors in Table) can be calculated based on the failure rate λ of each component and the test interval τ (i.e. 1 year = 8760 hours) as follows:

$$PFD_{avg} = \lambda \times \tau / 2 \quad (3)$$

The PFD_{avg} for the HIPPS function of BN model is calculated as 0.013107 according to Equation (1), which is the same as the result of RBD since assuming that the degraded working state has the same effect as fully working state on the failure of HIPPS

function. Another advantage offered by using BN model is to obtain the criticality of components by finding Most Probable Explanation (MPE) in BN model. It computes the probability of most likely configuration that leads to the system failure when the evidence is given. In this case, if the failure of HIPPS function is obseverd, the most likely explanation is determinted to be the failure of HIPPS valve, provided that other components can respond on demand. This could be explained as HIPPS valve has the highest failure rate and is connected in series.

This BN model can be itegrated with the Markov process if the repair action is taken into account to calculate the availability, where priors will be replaced by the steady-state probabilities of the corresponding states.

Table 1. Failure rate and prior probability of root variables

Root variables	Failure rate (per hour)	Prior probability
PT	0.3×10^{-6}	1.314×10^{-3}
Logic	0.1×10^{-6}	0.438×10^{-3}
Pilot	0.8×10^{-6}	3.504×10^{-3}
HIPPS valve	2.1×10^{-6}	9.198×10^{-3}

4.2 *Effects of subsea sensors drift*

The importance of condition monitoring that normally performed by sensors is essential to foresee failures under development and to make optimal interventions based on the prediction of remaining useful life. However, the industry has experienced that some sensors installed subsea are vulnerable to drift, an effect that will lead to reading offsets or the erratic reading of sensors. This may be a concern also for new sensors, despite new technology proposal to overcome this problem. In topside (dry) environment, the negative impact of sensor drift could be removed by some maintenance tasks like re-calibrations, but this is not possible subsea without retrieving the sensor. In this example, the sensor drift is considered as a contributing factor that can influence the success of 2oo3 voted system within different magnitudes, i.e. *High*, *Medium* and *Low*.

Various factors can influence the magnitude of the sensor drift, such as physical property of the sensors (e.g. usage) and various environmental factors (e.g. temperature and pressure). However, the cause-relationship between these subsea RIFs and sensor drift has not yet been fully captured in the subsea environment, as RIFs may vary with different design alternatives and operating environment. In this example, we tacitly assume that two RIFs, namely as 'RIF1' and 'RIF2', are relevant in estimating magnitude of drift of sensors.

In order to model this long term but slow degradation effect, some relevant assumptions need to be made as follows:

- The sensor drift introduced here is considered as the cause to the failure of PT voted system. This may be present in all three PTs at the same time, but the degree of drift can be different. Therefore, the number of functioning sensors can influence the probability of responding to a high pressure condition, meaning that fully working state and degraded working state have different impact on the system failure.
- The sensor drift starts after installation, and sensors will experience different levels of drift during each test interval. In this example, the sensor drift is assumed as discrete distributed in the early evaluation.
- The re-calibration may be done by software implemented compensation, using e.g. models ("virtual/soft sensors") combined with other physical measurements. But these modeling aspects of this option has not been included in the model here.
- The two RIFs can be disjoint (e.g. physical property (material) of sensors and temperature) or correlated (temperature and pressure). The statistical dependencies between selected RIFs can be incorporated according to Figure 1. In this example, the two RIFs are assumed to be disjoint. It is worth noting that the selected RIF can also connect to other nodes and such conditional dependencies can be easily accommodated in Bayesian formalism, e.g. material selection of sensors and failure rate of sensors.

The BN model that includes the sensor drift and associated RIFs is shown in Figure 5. The conditional dependencies between variable 'drift' and 'PT_voted' are presented in Table 2, where values of state 'faulty' of 'PT_voted'for all states of 'drift' are assigned as 0 then can be omitted. The value assigned in Table 2 can be explained as: the 2oo3 voted system has a probability of 0.015 to fail in the situation that only two PTs can respond and the effect of drifting is high. Table 3 contains the conditional dependencies between two disjoint RIFs and variable 'drift'. Note that H, M, and L stands for states of drift effect and -1, 0, +1 of RIFs means the associated RIF has negative effect, no effect, positive effect on the drifting. The value assigned in Table 3 can be explained as: the distribution of different drifting effect is estimated as [0.4 (High), 0.35 (Medium), 0.25 (Low)] under the situation that RIF1 has negative effect and RIF2 has positive effect. The values assumed in Table 2 and Table 3 in this example are only for the purpose of illustration.

The PFD_{avg} of HIPPS function is now slightly increasing from 0.013107 to 0.015345 after introducing sensor drift. For this case study, if the failure of HIPPS function is obseverd, according to the result of MPE, the HIPPS-valve is the most likely one to be

blamed. Therefore, one may conclude that: when the subsea HIPPS is influenced by sensor drift that is estimated in this example, the most vulnerable component is still the HIPPS valve until sensor drift reaches the pre-defined acceptable limit.

In this example, the values are assigned for the purpose of illustration. The priors of RIF1 and RIF2 are given as [-1(0.1), 0(0.9),+1(0.1)] and [+1(0.83), -1(0.17)], expressing what one (the expert) thinks about the probabilities of states of RIFs. The priors of RIFs can be determinted based on multiple source of information, e.g. (new) interpretation of historical evidences and operation experience. The values of RIFs be continuously updated if the new information is available, e.g. the (early) simulation result. If the failure of HIPPS function is observed during the test interval, the posterior state of RIF1 and RIF2 will be updated to [-1(0.08), 0(0.82),+1(0.1)] and [+1(0.42), -1(0.58)] representively, according to the Equation (2). Once the new RIF/failure cause/failure mode is revealed in the later phase (e.g. the prototype testing), it can be easily merged with the existing BN models by adding the casual arc or variables.

Table 2. Conditional probability between 'drift' and 'PT_voted'

	Drift		
	High	Medium	Low
Degraded working	0.015	0.01	0.002
Fully working	0.01	0.005	0.001

*The values in this table are assigned for illustrative purpose

Table 3. Conditional probability betweenm 'RIFs' and 'drift'

RIF1	-1 (0.1)		0 (0.9)		+1 (0.1)	
RIF2	+1 (0.83)	-1 (0.17)	+1 (0.83)	-1 (0.17)	+1 (0.83)	-1 (0.17)
H	0.4	0.1	0.15	0.05	0.1	0
M	0.35	0.2	0.05	0.1	0.15	0.01
L	0.25	0.7	0.8	0.85	0.75	0.99

*The values in this table are assigned for illustrative purpose

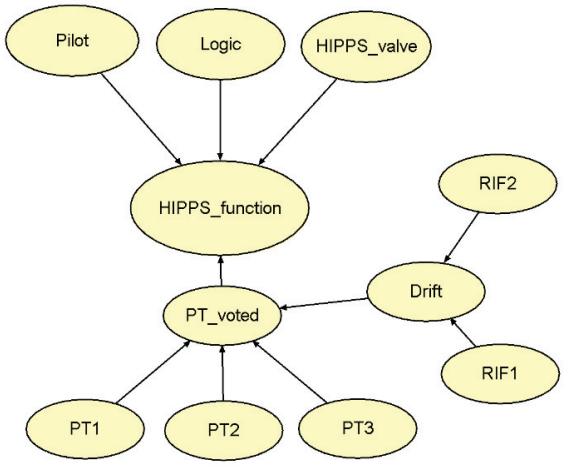


Figure 5. Two reliability influencing factors on the drifting

5 DISCUSSION AND CONCLUSION

This paper use an illustrative example to demonstrate how to incorporate the foreseeable operational conditions of future subsea design (e.g. drifting of new subsea sensors) and how RIFs that in an early design phase can be foreseen as important, by the proposed reliability model that adapting Bayesian formalism. The presenting approach can provide an 'approximate but more closed to reality' indicator that reflects the best knowledge in the situation, to prove that the subsea system can operate as intended. The preliminary estimation can be continuously renewed through the evidence collection from the different stages of development (referred to the simulation in the early design phase).

The reliability model could be either very simple or very advanced, depends on modelling strategy. The prelimary proposal in this paper is not 'complete' and can be further improved, as it is subject to the following limitations and assumptions:

- The proposal can accomandate uncertainty involved in the novelty by improving the flexibility (by removing some restrictive assumptions) when model the system performance. The effect of data uncertainty (e.g. assigned value of RIFs) can be outlined by introducing probability distribution to variables. The level of completness uncertainty is still high because of, e.g. the proposal only provides a rather simple procedure that depends heavily on the element of judgement to determine the conditional probabilities between RIFs and failure cause (i.e. sensor drift). But the proposal is still promising as the level of uncertainty will be reduced within the increasing understanding of system risks and performance in the later phase. One promising approach is to provide an algorithm that combines the different type of data and relevance of the observed data in the suggested method. Some initiatives about identifying the relevance between systems (topside and subsea) have already been taken by Rahimi and Rausand (2013). The similar algorithm can be adapted in presenting method and even in a more advanced way due to the probabilistic characteristic of BN model.
- Considering the wear effect of subsea equipment is important since no preventive maintenance work are carried out subsea. Encountering Weibull distribution to present the increasing effect of degradation (e.g. drifting) in the suggested method is an area where further work needed.
- The presenting approach has not been implement against a real case. Our suggestion for further research work is to investigate the

physics behind the sensor drift so that the realistic RIFs are selected. The sensitivity analysis should be performed to obtain the relative importance, the most important RIF can therefore selected to be included in the early evaluation of new subsea design.

ACKNOWLEDGEMENT

The authors gratefully thank to the support from the new center for innovation-driven research on Subsea Production and Processing (SFI SUBPRO). The author would also like to thank reviewers for giving comments to improve this research work.

6 REFERENCE

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into bayesian networks. *Reliability Engineering and System Safety, 71*, 249–260.

Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., & Bérenguer, C. (2010). Failure rate evaluation with influencing factors. *Journal of Loss Prevention in the Process Industries, 23*, 187-193.

Cai, B., Liu, Y., Fan, Q., Zhang, Y., Yu, S., Liu, Z., & Dong, X. (2013). Performance evaluation of subsea BOP control systems using dynamic Bayesian networks with imperfect repair and preventive maintenance. *Engineering Applications of Artificial Intelligence, 26*, 2661-2672.

Cai, B., Liu, Y., Liu, Z., Tian, X., Dong, X., & Yu, S. (2012). Using Bayesian networks in reliability evaluation for subsea blowout preventer control system. *108*, 32-41.

Durga Rao, K., Gopika, V., Sanyasi Rao, V. V. S., Kushwaha, H. S., Verma, A. K., & Srividya, A. (2009). Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliability Engineering & System Safety, 94*, 872-883.

HUGIN. (2015). *software version 8.2* http://www.hugin.com.

IEC61508. (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems. Part 1-7*. Geneva: International Electrotechnical Commission.

Innal, F. (2008). *Contribution to modelling safety instrumented systems and to assessing their performance: Critical analysis of IEC 61508 standard, PhD Thesis*. Bordeaux: University of Bordeaux

ISO/TR12489. (2013). *Petroleum, petrochemical and natural gas industries -- Reliability modelling and calculation of safety systems*. Geneva: International Electrotechnical Commission.

Jensen, F. V. (1996). *An introduction to Bayesian Networks*. NJ, USA: Springer.

Jin, H., Lundteigen, M. A., & Rausand, M. (2012). Uncertainty assessment of reliability estimates for safety-instrumented systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 226*, 646-655.

Johansson, C. (2013). *On system safety and reliability methods in early design phases, PhD thesis*. Department of Management and Engineering, Linköping University, Linköping, Sweden.

Jones, B., Jenkinson, I., Yang, Z., & Wang, J. (2010). The use of Bayesian network modelling for maintenance planning in a manufacturing industry. *Reliability Engineering & System Safety, 95*, 267-277.

Khakzada, N., Khana, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection, 91*, 46-53.

Long, D. (2012). *A Primer For Model-Based Systems Engineering*: Vitech Corporation.

Lundteigen, M. A., & Rausand, M. (2010). Reliability of safety instrumented systems: Where to direct future research? *Process Safety Progress, 29*, 372-379.

MIL-HDBK-338B. (1998). *Electronic Reliability Design Handbook*: US Department of Defense.

Rahimi, M., & Rausand, M. (2013). Prediction of failure rates for new subsea systems: A practical approach and an illustrative example. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability August, 227*, 629-640.

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. Hoboken, NJ: Wiley.

Rausand, M., & Høyland, A. (2004). *System Reliability Theory, Models, Statistical Methods, and Applications* (second edition ed.): John Wiley & Sons, Inc.

SINTEF. (2010). *Reliability Data for Safety Instrumented Systems - PDS Data Handbook, S.Hauge, T.Onshus (Authors)*: SINTEF.

Vatn, J. (2013). *Risk_OMT-Hybrid approach, Course PK8200-Risk Influence Modelling and Risk Indicators*. Norway: NTNU.

Framing Reliability Specification in Early Design Phase of Subsea Systems

---

Zhang J, Liu Y, Lundteigen MA. Framing Reliability Specification in Early Design Phase of Subsea Systems. *Presented at RQD2017, August, Chicago, USA*

Framing reliability specification in early design phase of subsea systems

Juntao Zhang[1], Yiliu Liu[1], Mary Ann Lundteigen[1]

1Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Keywords: Reliability, early design, subsea, systems engineering

Abstract - Incorporating reliability in the early stage of a design process is important to reduce the chance of overlooking functional requirements that, if not included, will require redesign at a later stage. Reducing such risk in early design phase relies on the ability of reliability analysts and designers to cooperate very closely. Key actors in subsea oil and gas industry have pointed out that available frameworks are not so detailed on *how* this can be achieved for novel and specialized products. The purpose of this paper is therefore to propose a framework for the handling of reliability in subsea design, and to suggest how to develop the reliability specification in close collaboration with the system design team. A novel subsea design concept is adopted as a case study to demonstrate the application of the proposed framework.

Introduction

RAMS is often used as a collective term to describe important and highly interrelated attributes of a given system or product: reliability, availability, maintainability/maintenance and safety. Incorporating RAMS in early design offers (at least) two benefits: (1) It raises new issues to consider in the evaluation of design concepts, beyond what are already identified by designer's own models and tools, and (2) it gives early indications of design concepts about life expectancies and intervention needs. However, traditional RAMS analyses may have their own limitations in the early design phase due to limited amount of relevant reliability data and failure information. Some may argue that reliability is the 'obvious' result as long as designers do their jobs properly. However, involving reliability analysts too late may result in costly modifications in subsequent phases, due to improper specification of how the system shall detect and respond to failures, how the system performance can be demonstrated prior to installation, and how the system can maintain its performance under changing operating environment. Controlling such risks relies on close interaction of system designers and reliability analysts when the early design concepts are being specified.

State of the art methods in the management of RAMS in early design phase are described in international standards like IEC 60300, for example [6] which focuses on reliability specification. It may be noted that this standard focuses on RAM only. Other standards like [7] concerns safety, which is also as a basis for other industry sector standards, such as [8] for process industry, [13] for aviation and [10] for automotive. The oil and gas industry has also developed frameworks for system performance in a wider context, such as [9] that covers a systematic program for ensuring a link between system performance and the performance of processing facility and distribution networks. Most manufacturers and system integrators of subsea systems have already internal procedures for managing RAMS in design, following the recommended practice [4] and [1]. Still, it is often mentioned in contact with industry that RAMS are not well integrated in the earliest design stages. One reason is that reliability analysts and system designers are not having sufficient level of interaction, and there is sometimes missing a clear link between models and specifications that designers use and the ones that reliability analysts use. For example, Failure Mode, Effects and Criticality Analysis (FMECA) is often suggested, and in some cases, this is the only tool used for communication between these disciplines during a design process. FMECA is a powerful tool, as it is easy to apply and understand, but at the same time it has its own limitations as it cannot encounter dependencies and common cause failure (CCFs). RAMS demonstration is also a vital part of the framework, and this part is still under development. [12] have pointed out some challenges associated with demonstration: the emphasis on quantification of reliability sometimes impede the transmission of failure information to designers who are not familiar with reliability theory. RAMS analysts often dive into demonstration before completing the full specification, due to limited time for verification process of project.

The current marketing situation requires new subsea units are both cost efficient and reliable, which requires extensive development and rapid introduction of new technology. For this reason, it is of vital importance to improve both the means of communication between designers and RAMS analysts, and the models being used to capture the subsea-specific challenges of adapting technology concepts to demanding operating environment and limited accessibility for regular maintenances.

This paper suggests a framework to complete the current industry practice. The main emphasis is placed on the process towards the specification of RAMS by incorporating design implications. The case study has been selected on the basis of systems being relevant for the research based innovation center for subsea production and processing [14]. The results are iterated through interviews and regular meetings with industry involved. The remainder of the paper is organized as follows. Section 1 gives the general consideration for RAMS analysis and design work, based on the iteration with industry partner and other projects inside SUBPRO. Section 2 illustrates the derivation of the proposed framework. Section 3 demonstrates the application of proposed methods within a simple subsea design. Section 4 presents the conclusion.

1. General considerations

Managing RAMS includes, beyond RAMS planning, the following two key phases: RAMS *specification*, i.e. the process of identifying the required and/or desired RAMS attributes, and RAMS *demonstration* that covers analyses (qualitative as well as quantitative) needed to verify that specified RAMS requirements are reasonably met. RAMS specification is an extension of the system or equipment *design specification*, with focus on the RAMS related requirements. An important attribute of the RAMS specification is to cover functions, beyond those being "obvious" from designer's own analyses and specifications. Such additional functionality may relate to provision of information (e.g. monitoring of technical state), allowance for testing (e.g. remote and diagnostics), protection of equipment, and behavior upon fault conditions. This paper aims primarily at framing of RAMS specifications, to close the gap between design specification and RAMS specification.

The term '*early design*' used in this paper refers to the specific phase of product development as shown in Figure 1. The focus of early design concept development is placed on the specification of system missions and relevant functions, but the implementation is not specified to sufficient level. Different existing methods are selected according to level of details. For example, interface FMECA is used later when interconnections of components are specified. However, the existing methods in RAMS fields have their own limitations, e.g. FMECA is often criticized for underestimating critical combinations of failures [4]. Instead of using FMECA solely, [13] recommend to use FMECA in together with Fault Tree Analysis (FTA) to overcome this issue.

It is not enough to specify required performance in response to fault conditions. RAMS analysts must also identify additional requirements relating demonstrating and maintaining RAMS performance once installed, considering how the system is to be tested, monitored, and prepared for replacement of critical items (if failed) during operation[6]. Qualification testing prior to system being installed, such as lifetime testing, may also call for special (and temporary) preparation. In the early design phase, the focus is placed on reliability modelling to get conservative reliability estimate, and the commonly used measure is Mean Time to Failure (MTTF). However, in most cases, the RAMS specification is not detailed enough to reflect the detailed physical system architectures. Instead, the RAMS analysts should aim for developing RAMS models that have a focus on functional and architectural relationships and constraints.

Both the design and the RAMS specification need to be updated in iterations, as both may pose a need for changes to the other. However, this interlink is not fully clear and well adopted in industry practices, and this may lead to extensive time and resource being wasted from the lack of proper communication. In this paper, a framework is emerged based on systems engineering, a concept for systematically managing system development and implementation, bridging designers (or users) efforts with the RAMS specification. The framework aims to reduce uncertainty in design and operation of subsea system, even with limited experience available at early stage. The following subsections will briefly discuss the interaction between tasks of systems engineering and RAMS, to ensure design constraints are reasonably reflected in RAMS specification.

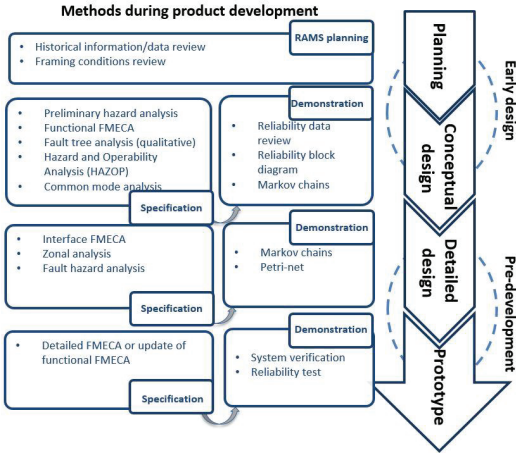


Figure 1. RAMS methods in product development process

2. Framework development

2.1 Holistic approach

The proposed framework is illustrated in Figure 2. The framework extends RAMS tasks in early design phase illustrated in Figure 1 by including design efforts. RAMS specification adapts the design concept as a basis to perform tasks stepwise to identify how the system can fail and recover. The joint tasks are the identified critical steps to give sufficient insight of RAMS specification. The framework is iterative in nature, and realized by *design implications review*. This joint task collects the results from critical steps and communicate to system designers to decide on necessary follow-ups: update the formulated requirement or revise design concept. All tasks and their purposes are specified in Table 1. The subsequent

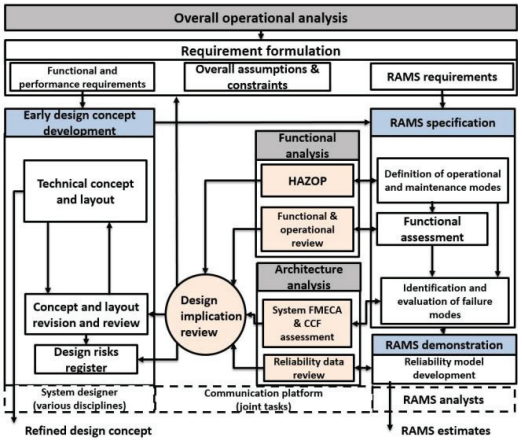


Figure 2 proposed framework

Table 1 Key tasks for proposed framework

Tasks	Purposes
Requirement formulation	-Systematically identify and document all requirements -Identify inconsistence in requirements
Definition of operational and maintenance modes	- Identify normal and abnormal modes of operation
Functional assessment	-Covers functions that are of highest interest to secure the reliability performance
Identification and evaluation of failure modes	-Integrate both failure information and a comprehensive set of influential factors, such as operational conditions during its in-service life and equipment specifications -Prepare for common cause evaluation
Reliability model development	-Choose suitable modelling formalism to capture subsea conditions -Identify relevant data and evaluate model capacity considering subsea issues
Functional and operational review	-Review identified functions and functional relationships
System FMECA and CCF assessment	-Carry out an extended/revised type of FMECA that is able to also capture common causes of failures -Demonstrate the possible evolution of the failure modes
Reliability data review	-Review reliability data available, including level of uncertainty. -Evaluate implications of lack of data, e.g. incorporate expert judgement
Hazard and operability analysis (HAZOP)	-Review systematically all system sections for abnormal operational situations for all modes of operations -Identify hazards and hazardous situations that must be encountered for or removed from design concept

subsection introduces how the systems engineering discipline can assist in specification of RAMS.

2.2 RAMS specification in proposed framework

The formulation of RAMS requirement for subsea system follows given framing conditions in related standards and regulation, e.g. [9] referenced in Petroleum Safety Authority (PSA). RAMS requirements are justified based on functional and architectural constraints.

Operational analysis defines ***why*** system is needed. Operational analysis is considered as the very first step to characterize the system, and covers many elements such as system missions and interaction with external systems. Operational analysis gives the global (even abstract) vision of system and its environment. The needs of detection and mitigation of failures arise the new element to be considered in the operational analysis, and further resulting in new functionalities and implementations. For example, maintenance activities are embodied by the interaction between system of interest and external supports, e.g. storage and mobilization of spare parts. The outcome of operational analysis is often the *requirement formulation.* When the RAMS requirement changes (e.g. system availability needs to be increased), we can therefore track down and make the necessary modification of design in time, and versa vice. The functional analysis defines ***what*** the system can do to meet the formulated requirement. RAMS specifications are directly linked to the functionality. Some functions to detect deterioration, e.g. condition monitoring (CM) or regular inspection and recourse for faults, e.g. activation of standby should be included in the *definition of operational and maintenance modes*. The commonly used functional analysis is often tree-like decomposition. However, this is not suitable for representing function dependencies. The full and complete *functional assessment* therefore should not only specify the input and output of system function, but also emphasizes on the functional dependencies. The block diagrams are in general suitable for representing interaction of functions, e.g. Function Flow Block Diagram (FFBD) recommended in [11].

The physical (architecture) analysis defines ***how*** the function is to be realized. In the early design where components are not specified, more emphasis is placed on the configuration and system structure. Most systems built for subsea are modular-design, where critical items with strong interactions but few interactions with externals are packaged together. Maintainability effort is only directed to the module level (rather than individual equipment), but the monitoring of technical states is allocated on component level. Therefore, the architecture dependencies should be included when formulating maintenance planning. Basic approaches of RAMS specification, e.g. FMECA or HAZOP, are sufficient for simple system that has limited complexity. However, for complex systems like a subsea system, the basic approaches cannot cover all necessary information, i.e. functional and architecture constraints and interdependencies.

3. Case study

A subsea boosting concept involving subsea Electrical Submersible Pump (ESP) system was selected to demonstrate the application of selected elements of the proposed framework.

3.1 Technology concept and layout

The ESP system has been a viable technical solution for boosting the pressure of well fluid from small fields and satellite wells [5]. One alternative of seabed application is to place the ESP in the horizontal section of a flow line jump that is used to connect subsea units [2]. This design concept offers the ease of intervention and minimizes the impact on existing subsea structure, since the deployment of pump assembly is the same as is done for flow line jumper.

The subsea boosting module is illustrated in the upside of Figure 3, and schematic of flow line jumper ESP that is sized to accommodate different well conditions is shown below. The mission of subsea boosting module is to boost the pressure of fluid and discharge to receiving facilities like manifold. The Flow Condition Unit (FCU) prepares the homogeneous mixture of gas and liquid before entering ESP inside the horizontal

casing. The electrical motor located on the upstream drives the centrifugal pump. The seal section is introduced between motor and pump to seal the dielectric lubricants within the motor and equalize the lubricant pressure with inside pressure [2]. The Liquid Collecting Unit (LCU) is designed to accumulate the liquid and part of liquid is recirculated to FCU. The instrumentations for temperature, pressure and vibration monitoring and communication cables for power feed are not illustrated in Figure 3. As of today, subsea industry tends to maximize the run life of boosting module due to the expensive mobilization of replacement or repair. The feasibility of subsea ESP is therefore evaluated from two points of interest: the size and capacity of ESP to accommodate the fact that composition of well flow may change over time, and RAMS attributes.

3.2 Definition of operational and maintenance modes

The result of operational analysis can be illustrated as a *context model* shown in Figure 4, where also stakeholders' (i.e. operators and those being involved in design, manufacturing and maintenance) influence on the lifetime of system is highlighted. This context model is then used to identify (in collaboration with the system designer) the operational and maintenance modes of ESP. The interaction between ESP and external systems includes e.g. (subsea) power distribution system and Remotely Operated Vehicle (ROV) for installation and retrieval. ESP can be switch to the operation of backup without stop production in presence of failures. Therefore, the availability of external systems is also needed to distinguish what is the 'hard' failures, i.e. requires shutdown, and 'soft' failures, i.e. compromising the production in an acceptable way (e.g. activation of backup). The complete operational scenarios analysis can provide sufficient information to complete HAZOP. Once the enough information has been gathered,

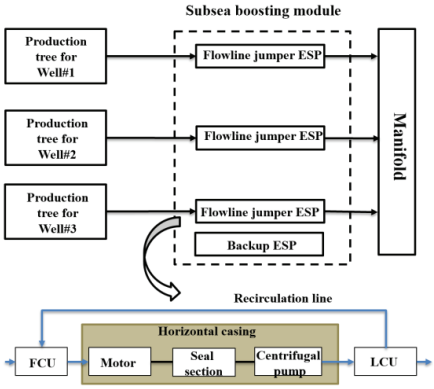


Figure 3 illustration of ESP in subsea boosting module

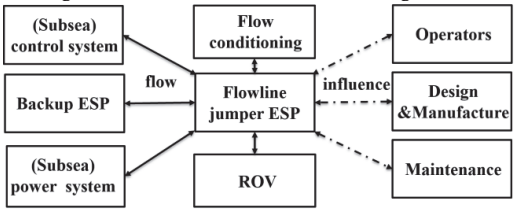


Figure 4 Flow line jumper ESP and its environment

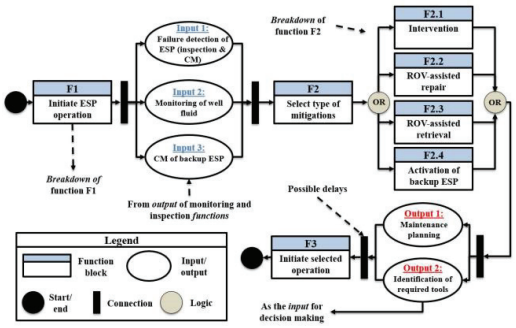


Figure 5 function model for fault response during operation

RAMS analysts have to focus on the follow-up functional analysis for each identified mode.

3.3 Functional assessment for the ESP

Figure 5 is a functional model used to illustrate how the ESP responds to failures during operation. The use of a backup ESP can add more flexibility to tolerate critical failures by temporary arrangement of configuration. Compared to a functional model of a single ESP, adding of backup arise the new need of monitoring (i.e. input 3) and devices for switchover (i.e. function 2.4). Each sensor (as the connection point) to a pipe can add the flexibility for detecting and replacing failed devices, but at the same time, they represent potential points to failures (e.g. leakage). Similarly, the activation of standby requires additional penetrating cables and jumpers, which increase the complexity and possibility of communication failures. The normal operation of ESP (i.e. function 1) can be further broken down to have the tree-like decomposition to indicate what function and related components are needed. It can be used as the basis to develop Boolean approach for reliability models, e.g. reliability block diagram or fault tree. The retrieval of ESP for repair or replacement is similar as the installation by using a lift line and ROV. However, the time required for maintenance planning and mobilization of spare part is often long (e.g. one month). It is often necessary to decouple the failure detection (i.e. input 1 and 2) and mitigation (i.e. Function 3). The possible delay of selected operation (i.e. Function 3) should be considered as one of constraints in subsea design, and this dependence should be accommodated in the advanced reliability model, e.g. Petri-nets with Monte Carlo simulation.

3.4 Identification and evaluation of failure modes

Identification of failure modes in the early design phase is often a daunting task, as very limited operational experience and data are available for new design concept. However, seabed ESP is not designed from scratch. Some components have already been approved for use in downhole (i.e. inside oil well) applications. The subsea environment and the technology novelty are recognized as culprits in limiting the seabed application of ESP. RAMS analysts should be aware that some architecture constraints are often overlooked in RAMS specification, such as size, weight and locations. This may arise one problem that some dependencies (whose presence may result in CCFs) are overlooked or underestimated. For example,

the downhole application of ESP is installed in the vertical position, but the subsea ESP is mounted in the horizontal section of jumper. ESP performance is now sensitive to the alignment and straightness. It is therefore necessary to specify the tolerable degree deviated from horizontal and identify possible compensating methods (e.g. rigid casing). The leakage in seal section can cause gradual contamination in neighbor areas, such common causes due to the proximity are generally evaluated in zonal analysis but in the later stage, see Figure 1 and also the discussion in [13]. In the early design, the failure effect on module or system level must be registered abstractly in system FMECA, to prepare for complete and full CCF analysis when schematic of design is ready. When discussing evaluation of failure modes, much attention is put on failure rate, but the origins of failure, i.e. influencing factors are frequently ignored. RAMS analysts are therefore responsible to integrate both failure information and a comprehensive set of influential factors, such as operational conditions during its in-service life and equipment specifications. The investigation on influential factors will also give the possibility for apply statistical method to estimate corresponding failure rate, see also discussion in [3].

3.5 Design implications review

For the early design of flow line jumper ESP, the main design implications are the testing policy and methods for backup ESP and investment in redundancy. The control system and monitoring devices of ESP are essential for flow line jumper ESP. However, the spurious stop, i.e. the unexpected shutdown may be caused by the errors of control and monitoring devices. The designers should be aware of the potential to compromise on production. Some strategies like 'shared-' or 'model-based' sensors should be considered when come to the detailed design. However, the effect of these strategies has not been fully captured when setting the reliability and availability target. This may require more qualification effort in the later stage. In addition, there will be very limited possibility to monitor the states of backup ESP since there is no flow through the pipe. System designer may consider having the bypass line connected the dormant backup system to perform the regular inspection or test when the main ESP is still in operation. All these identified issues are registered as *design risks*, and may make the system designer to have *design revision and review*.

4. Conclusion

It has become apparent that incorporating RAMS aspects as early as possible gives several advantages in form of engineering efforts and budgets. Many companies involved in subsea development have their procedures for managing RAMS in design but they still claim that they are not adequate. The existing methods and approach in RAMS discipline may not be able to give systematic insight of the design concept, so it is necessary to integrate other disciplines to complete such practice. This paper proposes a new framework, and the focus is placed on the 'communication platform' to integrate different disciplines and explore the potential of improving existing methods for subsea design. This framework therefore allows the proper consideration of RAMS when design decisions are made. The case study demonstrates the proposed framework used for a new subsea concept, where some key features of this new design concept are briefly discussed. The further step for improving this framework is to specify how to close the gap between RAMS specification and RAMS demonstration. In addition, specific elements of proposed framework are still subject to further development, by using piloted concepts developed as part of the SUBPRO research center as basis.

Acknowledgment

This work was carried out as a part of SUBPRO, a Research-based Innovation Centre within Subsea Production and Processing. The authors gratefully acknowledge the financial support from SUBPRO, which is financed by the Research Council of Norway, major industry partners and NTNU.

References

[1] API-RP-17N. (2009). *Recommended Practice Subsea Production System Reliability and Technical Risk Management*: American Petroleum Institute.

[2] Baker Hughes. (2007). *US patent 7565932: Subsea Flowline Jumper Containing ESP*.

[3] Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., & Bérenguer, C. (2010). Failure rate evaluation with influencing factors. *Journal of Loss Prevention in the Process Industries, 23*, 187-193.

[4] DNV-RP-A203. (2011). *Qualification of New Technology*. Høvik, Norway: DNV.

[5] Homstvedt, G., Pessoa, R., Portman, L., Wang, S., Gonzalez, J., Maldancer, M., & Margulis, J. (2015). *Step-Change Seabed ESP Boosting*. Paper presented at the Offshore Technology Conference, Brazil 27-29 October.

[6] IEC60300-3-4. (2007). *Dependability management - Guide to the specification of dependability requirements*.

[7] IEC61508. (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems. Part 1-7*. Geneva: International Electrotechnical Commission.

[8] IEC61511. (2003). *Functional Safety – Safety Instrumented Systems for the Process Industry*. Geneva: International Electrotechnical Commission.

[9] ISO 20815. (2008). *Petroleum, petrochemical and natural gas industries– Production assurance and reliability management*. Geneva: International Organization for Standardization.

[10] ISO 26262. (2011). *Road vehicles – Functional safety*: International Organization for Standardization.

[11] Long, D., & Scott, Z. (2012). *A Primer For Model-Based Systems Engineering*: Vitech Corporation.

[12] O'Connor, P., & Kleyner, A. (2012). *Practical Reliability Engineering, 5th Edition*. Hoboken, NJ: John Wiley & Sons, Inc.

[13] SAE ARP4761. (1996). *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. USA.

[14] SUBPRO. (2015). *Subsea production and processing*: https://www.ntnu.edu/subpro.

A systems engineering–based approach for framing reliability, availability, and maintainability: A case study for subsea design

Zhang J, Haskins C, Liu Y, Lundteigen MA. A systems engineering–based approach for framing reliability, availability, and maintainability: A case study for subsea design. *Systems Engineering*. 2018;1–17. https://doi.org/10.1002/sys.21462

Received: 28 June 2017 | Revised: 22 June 2018 | Accepted: 7 July 2018

DOI: 10.1002/sys.21462

RESEARCH PAPER

WILEY

A systems engineering–based approach for framing reliability, availability, and maintainability: A case study for subsea design

Juntao Zhang | Cecilia Haskins | Yiliu Liu | Mary Ann Lundteigen

Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, Trondheim, Norway

Correspondence
Juntao Zhang, PhD, Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, S. P. Andersens veg 5, Valgrinda*1.305C, Trondheim, Norway
Email: juntao.zhang@ntnu.no

Abstract

Framing reliability, availability and maintainability (RAM) aspects are critical for an engineering design, as RAM is concerned with the sustained capability of a system throughout its useful life. RAM analysts are responsible to consider both functional and dysfunctional behavior of a given system beyond the perspective of system designer. However, the system concept baseline developed by RAM toolset is often a partial view, which is either too abstract when preparing RAM analysis or too overloaded when integrating RAM analysis with design process. Such practice may not give systemic insights of the design concept, considering specific subsea design challenges such as limited accessibility and requirement for automate control. For this reason, it is of great importance to ensure an effective and sufficient communication between the domain of design and domain of RAM. Integrating with a well-known engineering discipline, such as systems engineering (SE), may help analysts to create the collaborative design environment necessary to control the design risks for a system with high complexity. This article proposes a new framework that links SE with RAM engineering by connecting relevant concepts and models used. A novel subsea design concept is offered as a case study to demonstrate the key changes in subsea design activities for addressing RAM with the proposed framework.

KEYWORDS

availability, reliability, subsea system, systems engineering

1 | INTRODUCTION

Reliability, availability, and maintainability (RAM) is concerned with the sustained capability of a system throughout its useful life. RAM plays an essential role in the engineering design process of subsea systems to create competitive advantages, such as reducing capital investment (CAPEX) and operational costs (OPEX), controlling the risk of redesign, and mitigating potential future production disturbances.[1] RAM of technical systems are receiving center stage attention in many sectors, such as automotive,[2] aviation,[3] nuclear,[4] oil and gas (O&G),[5] and railway.[6] RAM analysis based on feedback from existing legacy systems imposes constraints on systems requirements, architecture, and design.[7(p97)] However, managing RAM is often viewed as a separate activity in many subsea engineering practices, and the relationship to other established engineering frameworks, such as systems engineering (SE), are often not developed. For example, in discussions that have taken place inside the research center of SUBPRO[8] with manufacturers of subsea systems, we see that they have established both RAM and SE processes, although the tasks may not be coordinated and there is no well-established practice for how to share and use results across the two processes. One specific concern is that misinterpretations may arise due to the inconsistencies in backgrounds, jargons, and models used by the different engineering frameworks. This is a real concern in the O&G domain where a myriad of contractors and subcontractors must cooperate to achieve a final solution. Another, and perhaps even more important concern is that the SE and RAM engineering frameworks are not utilized at full potential to identify, address, and solve design challenges that involve new operating environments or new technology. Some research initiatives have been studied to resolve similar problems, such as concurrent engineering[9] and Design for Reliability (DfR).[10,11] However, concurrent engineering is more about coordination of technical engineering discipline, where the focus may not be placed on its interrelation to RAM engineering. DfR toolset mainly focuses on how to improve the design through complete testing and experiments carried out in later stages of design, where the analytical methods and modeling of RAM engineering receives limited attention. Our hypothesis, which forms that basis of the research in this article, is that it is necessary to integrate RAM analyses with SE analyses, to

holistically address the generally high complexity associated with technical systems.

The authors investigate and suggest a new framework to integrate RAM engineering with SE. The International Council on Systems Engineering[12] defines SE as "an interdisciplinary approach and means to enable the realization of successful systems." RAM engineering shares some similarities with SE. For instance, they both employ models developed to give an abstract view about system behaviors and physical configurations, albeit for different analysis needs. This article provides a view on how to make specific couplings between SE and RAM engineering in terms of concepts and models used. RAM engineering is often considered as a specialty subset of SE,[7] and even then it seems that the specific interfaces between SE and RAM engineering are given limited attention. The authors select some literature from the SE community and discuss the interrelationship with typical RAM analysis methods and steps. A new framework is proposed on basis of this evaluation, to mirror SE for extending the current practice of framing RAM aspects in design.

A review of the literature uncovered references that discuss the potential integration and proposes some tools to support exchanges between RAM and SE. Jigar et al[13] presented ways to extend the existing availability allocation process to the relevant stakeholders involved by applying a SE approach. The work indicates that the availability allocation problem can be redesigned within SE principle, so that the analysis is conducted in an iterative and systematic manner. Garro and Tundis[14] showed the possible extension of reliability analysis of a system to that of the System of Systems (SoS) concept, to solve the main issues arising in system reliability analysis considering particular properties of SoS. Leveson[15] proposes the new accident model based on systems thinking, that is, Systems Theoretic Accident Model (STAMP), where the safety problem is reformulated as a control problem thus make greater progress toward safety analysis of complex system. Shainee et al[57] apply SE to the design of a technical marine SoS, while Ramírez et al[56] discuss ways that SE serves in coordination and communication by alleviating potential friction between multidisciplinary actors.

This article uses a subsea O&G production system to explain the foundation of the framework and demonstrate its applicability. Due to lower oil prices and changing field conditions, the Norwegian-based O&G industry is increasing the installation of subsea equipment to accommodate pressure assistance, O&G separation, and water treatment.[16] The *marinization* of topside technology (eg, fixed or floating facility) offers several benefits, such as increasing recovery from the field and saving costs associated with manning and maintaining the platforms. Hereafter, such innovations for improving current production solutions are referred as *new subsea design*. As of today, manufacturers and system integrators of subsea systems use internally developed procedures for framing RAM in the design, following standards such as ISO 20815[5] that link production assurance with reliability management in a wider context, and more detailed recommended practices such as DNV-RP-A203[17] and API-RP-17N.[18] However, the current practices are not optimized for recognizing new and specific design challenges or new operating environments. For instance, failure mode, effects and criticality analysis (FMECA) is often used as "one size fits all" method for failure analysis, regardless of whether systems are installed subsea or topside. In the proposed framework, we will discuss how outdated practices can benefit by using SE methods as a foundation.

Subsea Production and Processing (SUBPRO) is an initiative funded by the Norwegian Research Council to address current and future challenges in subsea systems that require multidisciplinary collaboration. The project combines researchers and industry partners to address the gaps in knowledge and accelerate the level of innovation in O&G field development and operation.[8]

The rest of article is organized as follows. Section 2 explains some of main characteristics of a typical design processes within SE and RAM, including highlighted similarities and differences. The new framework, referred to as RAM-SE, is introduced and explained in Section 3 and followed by a presentation in Section 4 about how these two discipline get advantages from such integration. A new subsea design concept is presented in Section 5 to demonstrate the application of the proposal. The case study has been selected on the basis of systems relevant for the research based innovation center for SUBPRO. A summary with concluding remarks and suggestions for future research is given in Section 6.

2 | RAM ENGINEERING AND SE

The following subsections give a brief introduction to the practice of RAM engineering and SE, including general considerations and practical challenges with respect to new subsea design. The discussions and reflections are based on literature review, investigation of the current industry practices, and feedback received from participants in the research project SUBPRO.[8]

2.1 | RAM engineering

RAM engineering aims at using engineering knowledge and techniques to control the risk of failures and reduce engineering uncertainties.[19] The main activities of RAM engineering covers (a) artificial experiments to test out the properties of a given system or parts, and (b) analysis and modeling techniques to reveal the cause-effect relationships between failure and specific conditions.[20] Activities, such as life time testing, carried out later, are of little relevance for this article and thus will not be further discussed.

Figure 1 gives some state of art methods for RAM analysis at different stages of a design process, based on discussions by Bertsche[21] and Johansson.[22] RAM analysis identifies issues to consider in the evaluation of design concepts, beyond what are already identified by the designer's own models and tools, such as provision of information (eg, monitoring of technical state), allowance for testing (eg, remote and diagnostics), protection of equipment, and behavior upon fault conditions. RAM analysis can be both qualitative and quantitative. Qualitative analysis is used to identify failure modes, mechanisms and causes (such as FMECA), and determine the possible maintenance and test strategies. Probabilistic analysis uses the result of qualitative analysis as the basis to quantitatively execute the comparative evaluation to support follow-up decision making. With the design evolution, these

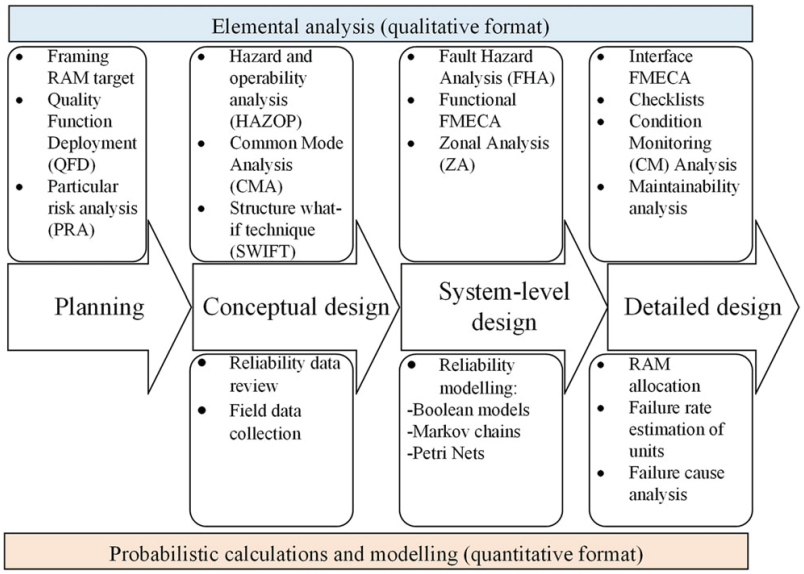


FIGURE 1 Mapping RAM methods in design process

analyses may be iterated, and updated via communication and consultation with operators, manufacturers, and designers.

However, the current process may not be optimal for complex system design. Highly complex systems are characterized by highly coupled parts and nonlinear interactions.[23] Unfortunately, alone many RAM methods in Figure 1 are not well suited for identifying and studying the effects of these interactions. Using them in this way introduces design risks that stem from insufficient considerations of engineering aspects, and will be latent on the first day of operation. The traditional RAM models follow *reductionism* (or analytical reduction), which fosters a *bottom up* approach by assuming that parts are operated independently and are not subject to feedback loop and interactions.[15,23] Such "system concept" developed by RAM analysts is not efficient for a complex system, as the hierarchy structure does not explicitly express any dependencies. Taking subsea as an example, high-level complexity is introduced by modular and compact design, software implementation (programmed functionalities), digitalization for communication technologies, interconnected hardware devices, and use of new technologies under more demanding (eg, autonomous) operating environment. These issues require efforts to systematically manage complexity, otherwise the framing of RAM aspects could be incorrect.

In addition, the heterogeneity of the multidisciplinary context in the design phase also restrains the use of current processes. System designers (who are responsible to organize system models considering various engineering disciplines at stakes) may have conflicting interests with RAM analysts, reflected by inconsistency of their models and focus of their elaborations. New subsea design is a concurrent and collaborative process, where different engineering teams are involved including RAM analysts. The RAM issues for new subsea design must be considered as early as possible to support decision making about redundancy, modularization, strategies for interventions, and the like. However, the effect of RAM considerations is not easily observed by other engineering teams, as confirmed by O&G industry partners who indicate that RAM analysis is not fully and actively used to support new subsea design. This said, many of the abovementioned methods do not have a well-defined interface with other analyses carried out in parallel phases of the design. A similar problem is also identified by Barnard[24] who points out that the overemphasis on probabilistic modeling frequently leads to misinterpretation of RAM analysis, which can lead to bad design or waste of engineering efforts.

For instance, a successful FMECA depends on a clear understanding of system concepts.[25] However, in practice one may start FMECA without establishing the holistic vision, due to the limited project time or independence of RAM analysis in the design process. The approach itself is unable to deal with critical combinations of failures modes, which means the failure or deviation is only analyzed individually within local perspective.[17] In the case of novel or unproven design, such as a new subsea design, many failures are systemic rather than the result of individual parts degradation, in particular for systems where software and communication technologies are used to implement a majority of the functionality. Systemic failures include "one of a kind" errors caused by improper operation procedure, software errors and flawed controls, and whose effects are complete or partial loss of functionality. Such failures may not be sufficiently identified through FMECA, which relies on a well-defined understanding of how the system can fail and the effects of failure. Therefore, the effect of failure at a system level is studied only partially. On the other hand, FMECA may take on a too large scope covering many trivial cases, which limits its support for decision making in design process.[26] It is therefore not ideal for engineers with different backgrounds to capture the useful concepts in their own models and analysis.

Table 1 summarizes some of the challenges of old practices in RAM engineering and indicates what we have suggested as requirements to a new approach. A relevant candidate to support the realization of

TABLE 1 Foundations for new practice of RAM engineering

Some typical errors in the old practice of RAM analysis	New requirements toward RAM analysis for complex design
Some engineering aspects may be ignored or misunderstood. Example: System familiarization is often subject to the competence and experience of RAM engineers instead of designers	Need to master complexity of design concept in a systematic and organized way before any specialty analysis.
The interactions between components/functions are not sufficiently considered in evaluating RAM performance. Example: The failure effect is only identified and evaluated on the selected hierarchical decomposition. The maintenance activities are evaluated in similar fashion.	The loss of RAM performance is beyond a chain of events. Need to organize the interactions between components/functions of system so the effect of failure is well understood.
The results of RAM analysis could be misinterpreted or misunderstood. Example: Probabilistic methods dominate in most practice. Human errors, software reliability, and systematic failures are not sufficiently covered in such analysis.	Need to communicate the result of RAM analysis in other ways than probabilistic based indicators so that systematic failures can be correctly communicated.
(Model-based) RAM activities are often "disconnected" from design process or have little interface with other engineering disciplines. Example: Heterogeneity in knowledge base	Need to integrate RAM engineering with other engineering disciplines involved in design process by connecting the produced models and used concepts.

these requirements has been identified within the SE framework. SE includes methods to support design team coordination, ensuring that the system concept is communicated correctly and that the correct system concept is communicated. SE also includes analyses that can improve the basis on which the RAM analysis is carried out.

2.2 | SE in subsea design

The core of SE is to apply system thinking to solve complex problems, where problems are viewed holistically instead of individually.[27] SE provides an iterative and systematic approach for problem solving, although the definition of SE varies across the literature.[28,29] The SE concept can apply to many industries to systematically analyze the given complexity, given two assumptions.[15] The first assumption is that the engineering effort for improvement on an individual component may not lead to an overall optimization. Returning to the subsea case, some subsea equipment cannot be replaced without pulling a whole module. This means that the effect of failure is not isolated to one component and one system function alone, but may include many others as well. Therefore, the individual improvement on component reliability may not improve the overall RAM performance. The second assumption is that the performance of individual component cannot be understood without considering internal and external interactions. For instance, subsea operation involves a high degree of automation and process control as manned actions have been dramatically reduced or eliminated in the subsea environment. This implies some errors are related to inadequate operation, flawed control process, and missing or wrong interactions. Analyzing failure caused by physical degradation is no longer considered as sufficient practice for framing RAM aspects on new subsea design.

This said, SE takes a lead role in organizing complexity for many disciplines including RAM engineering. Model-based SE (MBSE) suggests the use of models to support the view of a system concept. The system concept can be viewed from different perspectives, with the support of a rich set of model notations to capture the operational, functional, physical/architecture aspects of the system being evaluated. The traits of these models are briefly discussed in previous literature.[30–32] System Modeling Language (SysML)[33] is a commonly accepted technology for MBSE, which uses the same profile mechanism as Unified Modeling Language (UML) with some extensions made to give support to SE activities like requirement allocation. In this article, SysML is considered as the example SE tool for developing system architecture views.

Supported by a consistent system concept, one can eliminate the inconsistencies and misinterpretations caused by maintaining two sets of artifacts from the analysis of RAM Engineering and SE. Therefore, the pursuit of integrating RAM concepts along with the design process is realized by transferring between SE artifacts to analytical methods that solve the RAM-related problem. Figure 2 presents a conceptual map of these two types of models and the design itself. A SE artifact is a set of models that capture different levels of abstractions (ie, operational, functional, and architectural) of design, where RAM models inherit the same view with adjustments made due to accommodate the selected mathematical framework. Using RAM techniques or tools to construct the system concept may not be efficient as most of them are based on an error-prone point of view. SE models should be a prerequisite for developing a RAM model, and the consequent implications of RAM model influence the development of design concept by incorporating RAM aspects that extend most of design models based on SE tools.

3 | APPLYING SE TO INTEGRATE RAM IN SUBSEA DESIGN

This section will elaborate on SE activities with an outlook on RAM integration.

3.1 | Requirement analysis

The SE engineering process starts with identifying the requirements of stakeholders.[7] A complex system often involves multiple disciplines and is verified by multiple analyses rooted in different domains. The stakeholders can be classified based on their contributions as "primary," "secondary," and "tertiary."[34] Both RAM analyst and system

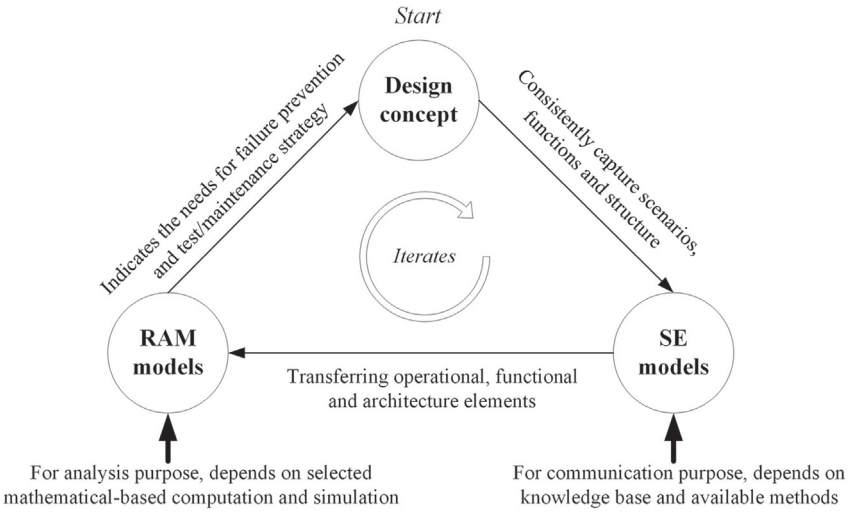


FIGURE 2 A conceptual map of RAM and SE models

designers who maintain a unified vision of the system concept are the primary stakeholders in new subsea design.

The glue that integrates the different contributing teams is the system level requirements that allow useful design concepts to be generated.[15] The study of operational concepts provides a preliminary overview to describe system missions, operating environment, and the internal/external interfaces. The typical models used for capturing a conceptual architecture are *operational context model*, *sequence diagram*, and *use case diagram*. The results of operational analysis are used to formulate contractual requirements. For example, with SysML one can model the text-based requirements supported by these diagrams together with a requirement table to clarify their relationships in the design.[35]

Much of the effort of a system designer is devoted to the functional requirements that define the behavior of system for fulfilling the needs, whereas RAM engineers aim to specify required RAM performance under different operating conditions. RAM requirements would be meaningless unless use profiles, environmental conditions, and operating conditions are specified.[36] The distinction between functional requirements and RAM requirements are important for eliminating inconsistencies between contributing engineering teams. Fulfilling the functional requirement does not implies the satisfaction of RAM requirement. The introduction or update of RAM requirements needs to update functional requirements and vice versa, but there are many constraints, for example, schedule and budget, on the simultaneous updates. In the context of subsea design, such conflicts can end up being more problematic, as most equipment and their interconnection cannot be modified after installation subsea. Therefore, it is more important to identify a *best* RAM performance considering the constraints of the operation and environment, rather than the theoretically *optimal* RAM performance. For example, the duplication of critical components (ie, redundancy) may add more flexibility in long-run subsea operation, but this decision implies costly installation and intervention due to the hiring of a larger vessel (ie, larger CAPEX).

The design should proceed with respect to these constraints and requirements to analyze functions and physical structure. Subsection 3.2 presents system architecture analysis as one of the most important SE activities and identify the role of RAM within.

3.2 | System architecture and analysis

As stated above, RAM engineers are accustomed to focus on the hierarchical function structure, since failure can generally be described as the termination or loss of functions and each function could be analyzed independently. Such practice is suitable for a system with simple interactions, decoupled functions, and straightforward part-function relationships, but not complex systems. Complex systems are better served by the SE suite of tools to systematically develop a vision of behaviors, interfaces, elements, and control structure for a new subsea system.

3.2.1 | Functional (behavior) analysis

Functional decomposition as a *static* representation of the hierarchy structure of functions is often adopted by RAM analysts to become familiar with the system concept. However, the tree-like decomposition with a local perspective cannot give the systemic view showing how the functions are coupled. The dependencies are not explicitly highlighted in functional decomposition.

In the SE community, different types of functional models are categorized as *flow-based* and *event-based*, and their representatives in SysML are *activity diagram* and *state diagram*, respectively. As a specialized form of flowchart, the activity diagram uses "tokens" to illustrate the concurrency of flow of control and data. This semantic aligns the structure of activity diagrams with that of Petri nets accepted in RAM community, although the activity diagram is more concise than standard Petri nets, especially when it comes to modeling the reactivity of workflow.[37] Considering the needs of quantitative notations, different mapping methods are proposed to translate UML activity diagrams to

Petri nets[38] or SysML versions.[39] The state diagram (or state machine diagram) explicitly describes the dynamics of an object or system. It consists of potential states and triggering events that drive the transition between states. The state diagram resembles Markov chains, perferred in RAM community on the surface, but with the distinction that Markov chains as the formal model based on strict mathmatical framework represent less content state diagrams. For instance, when transferring a state diagram to Markov chains for quantitative modeling, sychronization and parallelization of state diagram are abstracted away. The flow-based functional model and the event-based model are intended to be consistent; that is, if all transitions on a state diagram can be triggered by the completion of activities, then the context captured in activity diagram and state diagram are consistent. Activity diagrams based on flow of control are better used for modelling a process of operation, whereas the state diagram emphasizes events.

They are other models that are not covered in SysML that also support functional analysis. For example, the Function Flow Block Diagram (FFBD) represents the control structure and emphasizes the sequence of a successful operation. It is often implemented in conjunction with other models, such as N-squared diagram, in order to encompass all details of behavior.[32,40] In similar fashion, these graphical notations ease the communication of conditional system behavior between designers and RAM analysts even when no corresponding methods are found in RAM community.

Solely relying on functional architecture to analyze RAM performance of complex systems could be superfical and incomplete, as it only assists in identifying potential failure and repair events but not the associated cause and consequence. Therefore, the physical architecture of a design concept should be developed.

3.2.2 | Architecture (physical) analysis

The physical (architecture) analysis defines the components that realize the identified functions. Depending on the role RAM analysts have in the design phase, a technical system is generally considered from a functional instead of architecture point of view. However, it shall not be the case for new subsea design. Even if the well-rounded functional analysis is completed, we may not be able to evaluate the potential failure modes due to the incomplete view of given system concept.

The most commonly used approach to study physical aspects of system is the physical decomposition, which is often used as the "checklist" for the dysfunctional analysis, such as physical FMECA. However, such breakdown structure does not help in the context of complex system as many parts are interrelated and ought not be analyzed individually. Often times, studying physical aspects in RAM community is a brainstorming process that requires participations from multiple disciplines, for example, Hazard and Operability analysis (HAZOP). Few methods are proposed to exclusively incorporate physical properties in framing RAM aspects. Pioneering works have been encountered in the aviation industry, where the method zonal analysis is proposed to highlight the impact of proximity in Common Cause Failure (CCF) modelling.[3] Zonal analysis have not been fully exploited in O&G sector yet, but we can foresee this approach is meaningful as subsea modules are designed compactly thus the combination of effect of local failures or unwanted events may generate the potential hazards or increase the stress on the other components due to proximity. For example, the leakage of a pipeline can cause gradual contamination in neighboring areas. Such effects must be considered in some RAM methods for evaluating the failure rates upon environmental stress or other influencing factors, using analysis tools such as cause-effect diagram or Bayesian belief networks.

Using SysML, one can generate block definitions that contain physical attributes such as weight and size and they can also inherit attributes from other (higher-level) blocks. In such practice, building physical models of a subsea system can ensure coverage and traceability of defined constraints and assumptions (eg, height, width, mass, and the like). However, relying on the requirement table provided in SysML only gives an indication about constraints. The lack of 3D model can be compensated by using computer-aided design tools when needed. The complete architecture analysis can assist in understanding how the local effects on basic components can disturb the system and updating stochastic descriptions of unwanted events, together with expert judgments and experienced practices, for example, using finite element method to study the failure rate of a pipeline considering the effect of sand, fluid composition, ambient temperature, and pressure.

Additional attention should be paid to system structure, that is, the modularity in subsea design environment. Modularity deserves attention even in the early phase of subsea design, and can be illustrated as shown in Figure 3. Some subsea functions are realized by components located within different modules, but the replacement takes place at a module level.

Design structure matric (DSM) is rather a straightforward modeling technique to handle the modularity replacement problem.[41] The component-based DSM is often adopted in SE even though it is not available in SysML and here recommended for new subsea design. DSM is efficient in organizing the interactions between components and visualizing the shared patterns, and it can help designers to identify the relatively independent modules, and support some tasks such as RAM allocation.

3.3 | Trade-off analysis

Multiple conflict objectives are typical in an engineering design process. For example, the choice of materials to guard against internal corrosion in a pipeline may improve the reliability but may reduce the efficiency of production (ie, OPEX). Decisions are needed to find a balanced solution considering all the assumptions and constraints.

Trade-off analysis is ideally suited to the preliminary RAM analysis, and iterated for several rounds before finding the best possible solution. The relevant techniques for trade analysis have already been discussed in Refs. 42 and 43. Inputs from RAM analysis to trade-off analysis are ideally based on the methods mentioned in Figure 1. However, one should remember that quantification of all the factors identified in the dysfunctional analysis is nearly impossible. Establishing a set of scenarios (eg, accidental scenarios and maintenance

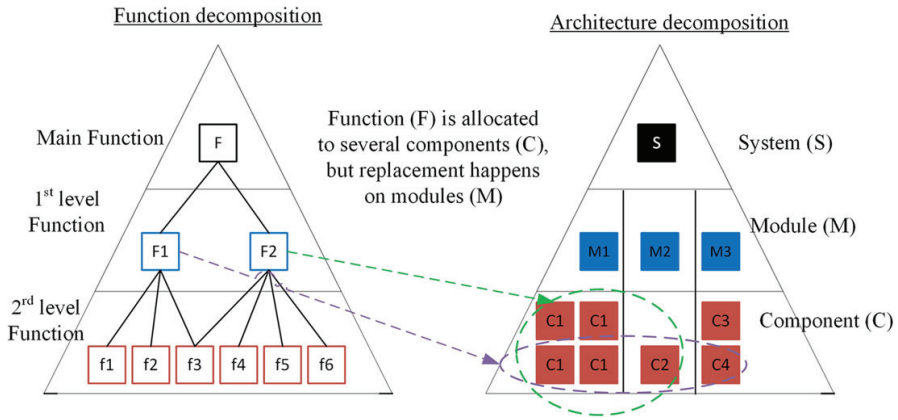


FIGURE 3 Modularity of subsea design

scenarios) is always considered as the supplement to communicate the implications on design. The subjective judgments are largely implemented in such analysis.

4 | RAM-SE FRAMEWORK

This section proposes a new step-wise framework for supporting RAM engineering in new subsea design. The proposed framework, shown in Figure 4, has been named RAM-SE. The RAM-SE framework revisits the current process of framing RAM aspects as given in Figure 1, and proposes several steps integrating both the SE and RAM community.

1. Step 1: *Operational analysis*. The operational analysis introduced here takes place alongside requirement analysis introduced in Subsection 3.1. It covers the identification of interactions, environment, and boundaries of the system for an overall view but offers only an abstract conceptual view of the design. The main objective is to systematically formulate RAM and functional requirements of a system, based on the needs of identified stakeholders.
2. Step 2: *Design analysis*. Hereafter, we use the term *design analysis* to cover both functional and architectural analysis introduced in Subsection 3.2. Design analysis assists in the systematic establishment of the design concept and supports the effort to understand and organize the system structure. RAM-SE uses often-cited methods from the SE community to establish the system architecture. The advantage for having design analysis is to efficiently eliminate the inconsistency caused by the variations in competence, knowledge base, and experience of RAM analysts. The highlighted methods in Figure 4 only consider subsea design environment. The refinement and complement of tools for design analysis should consider following criteria: system complexity and novelty, commonality, availability of software-based tools, plausibility, as well as the correspondence to RAM tools.
3. Step 3: *RAM analysis*. As opposed to the static system structure formulated in design analysis, RAM analysis focuses on the "dynamic" changes within the system structure. Table 2 summarizes the main objectives of the methods included in RAM-SE, and specifically discusses the possible extensions based on systems thinking. After defining the static system structure that explains how the components are distributed and connected, RAM methods are reorganized to simulate how the potential occurrences of events (eg, failure, test, repair…) affect the states of the structure (eg, parts, modules, configuration…). As always, the proposed methods in the framework should be updated or replaced based on the real analysis of needs.
4. Step 4: *Joint concept analysis*. This step is beyond the scope of Figure 1 but an important step that helps ensure sufficient interfaces between the design analysis and RAM analysis and appropriate follow-up actions. This analysis requires the involvement of RAM analysts and designers to accumulate results from discipline-specific analysis and decide on necessary follow-up based on the design implications of analyzed results. Some scenarios generated by RAM analysis may imply modifications of the existing design concept. Constraint-based trade-off checks whether the recommendations made based upon the results of RAM analysis are economically, technologically, and operationally feasible. For example, lifecycle cost analysis, sensitivity analysis, and technology evaluation must be conducted in this step.
5. Step 5: *Communication*. The communication block is centrally located to indicate its importance during all steps of RAM-SE framework. Communication is indispensable to link the separate contributions of design teams. The multiple players involved in the design process must agree on the "disagreement," and *continuously* evaluate the proposals from others. Effective communication should take place to ensure that all stakeholders understand the basis on which decisions are made and the rationale behind. Then the system concept configuration baseline should be based on both the contributions from RAM analysis concerning potential occurrence and damages, and trade-offs related to the system structure formulated in design analysis. Every revision should be registered as a *design risks* until it is validated.

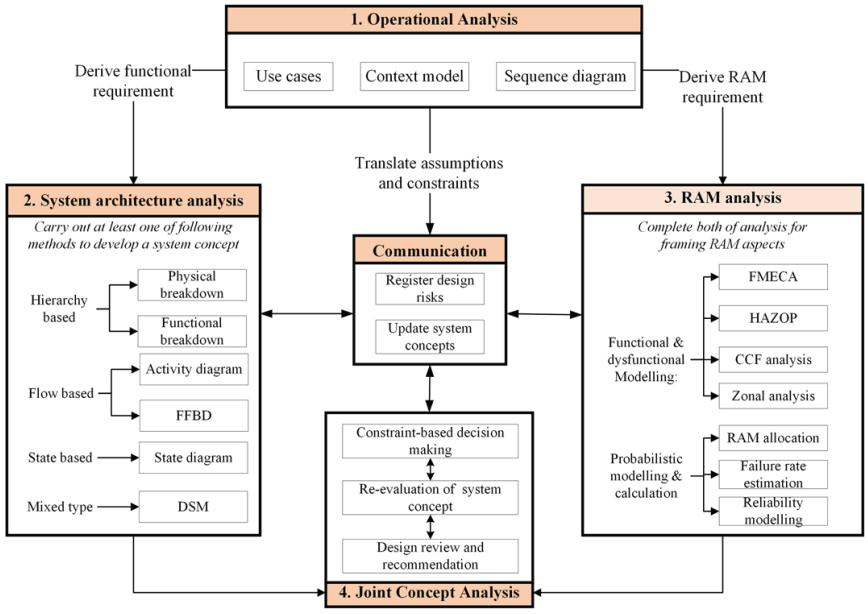


FIGURE 4 RAM-SE framework

5 | CASE STUDY

This section introduces an existing design concept-fiscal metering system. Adaptations must be made considering subsea specific issues.

5.1 | System description

The fiscal metering is one vital part in O&G sector to precisely measure petroleum product exported from delivery to the eventual recipient, a schematic is given in Figure 5. The accuracy and validity of flow measurement are very important for contractual obligation between custody transfer parties (eg, consumer and supplier). Statoil[44] has proposed a design concept for subsea fiscal oil export system using ultrasonic flow meter (USM). The main advantage is that USM has no moving parts so the maintenance requirement is rather low. Figure 5 presents the schematic of this design concept that consists of sampling module and metering module. The sampling module includes sampling devices (QS) and pumps. When the oil exported from subsea storage passes the sampling module, a representative amount of oil is extracted by sample probe. The pumps are installed to provide sufficient power for lifting the sample to the dedicated facility located topside via umbilical. The metering module consists of USMs, pressure transmitters (PT), and temperature transmitters (TT). When the oil is routed into pipeline of metering module, the volumetric flow rate, pressure, and temperature of flow can be measured. USM, QS, PT, and TT can be duplicated for backup use and improvement of monitoring capacity. In this design concept, one metering run contains a duty USM, a master USM, and a spare USM installed in series. The installation of multiple USMs enhances the ability of monitoring the quality of meters and reduces the measurement uncertainty if the resulted measurement is the average of readings from different USMs. The spare USM serves as redundancy to both master USM and duty USM. The metering module is considered as fully functional when two flow meters are available, where the spare meter can serve as duty or master when needed. The control system is located on topside to control the operation of sampling module and metering module. Subsea electronic unit (SEU) is installed to distribute the necessary coded control command to each instrument and collect the data for further transmission to other subsea units or control system. Assuming that duplicated SEUs are installed in the metering section to ensure the long-term stability, all the equipments are connected to two SEUs, so that there are redundant communication passes for metering station.

The validity and accuracy of signals from USM, PT, and TT may lessen after installation due to various factors such as outdated calibration, bad piping conditions, and physical damage of parts. This design concept is assumed to function in spite of failed PT and TT, since the loss of pressure and temperature measurement can be compensated by other transmitters adjusted by calculations. When there is a need to replace the USM, the metering station should be lifted through the rig and recalibrated at the accredited calibration laboratory. Replacement of USM causes an interruption of production as the downtime of metering station is significant.

This design concept includes many parts including PT, TT, valve connection, and tubing that have been qualified for subsea applications, except the USM. The following presents the evaluation of this design concept following the key activities in RAM-SE framework, where the main focus is directed to RAM performance of this design concept and necessary adaptations considering subsea conditions.

TABLE 2 Advancements for RAM methods in SE context

Methods	Objectives	Improvement by SE methods
FMECA	• Uses a basis for detailed RAM analysis and maintenance optimization and planning. • Document the effect of failure on system.	• Systematically identify all operational modes and functions attached to each potential failure modes. • Carry out an extended/revised type of FMECA that is able to involve dynamic aspects of key scenarios, see also the discussion in Ref. 52.
HAZOP	• Review all system sections for abnormal operational situations for all modes of operations. • Identify hazards and hazardous situations that must be encountered for or removed from design concept.	• Be less resource and time consuming. • Instead of brainstorming, focuses on the solid system architecture to evaluate the possible hazardous situations.
Maintainability analysis	• Establish maintenance strategies before put into the operation.[53]	• Incorporate operational and maintenance mode in the design analysis. • Develop the subsea system-specific or module-specific maintenance strategies.
CCF assessment	• Encounter common mode errors that lead to the loss of independence.	• Systematically indicate the possible dependencies among functions and system architecture, such as proximity, overlaps in functionality, and dependencies on resources (eg, data, information, and power supply).
Zonal analysis	• Encounter the malfunction that could result in serious effects on the adjacent components.	• Benefit from building a consistence system architecture that incorporates physical properties.
RAM allocation	• Decide the necessary improvement on component level to achieve the minimum required RAM performance in an optimal way.	• Benefit from building a consistence system architecture that considering modularity or other architecture aspects that may influence the efficiency of component improvement, for example, DSM.
Failure rate estimation	• Provide failure rates and other input parameters for reliability modeling and calculation.	• Integrate a comprehensive set of influential factors on identified failures brought up by design analysis. • Involve subsea designers as the experts via joint concept analysis for judging upon some particular issues, such as the excess of working loads, variations in internal or external pressures.
Reliability modeling and calculation	• Prepare a set of suitable models to be used for reliability and availability analysis. • Identify relevant failure scenarios and evaluate model capacity in light of these.	• Identify the characteristics of architectures (eg, modularization, obsolescence, and degradation) and scenarios/events (eg, delay on repair, imperfect testing or harmful testing, failures of activation of backup) needed to be considered in suitable modeling approaches.

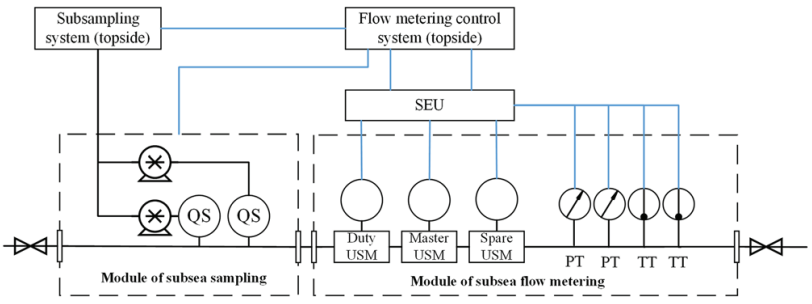


FIGURE 5 Subsea fiscal oil export metering system[44]

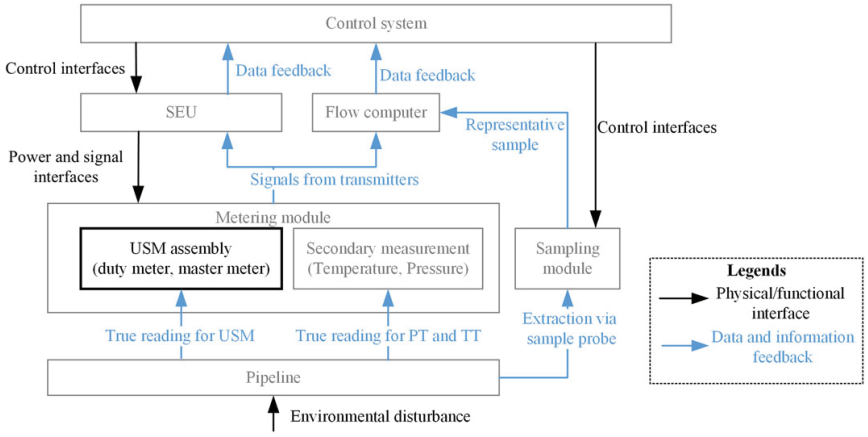


FIGURE 6 Context model for design concept

5.2 | Operational analysis

As shown in Figure 4, operational analysis frames the scope and paves the ground for both design analysis and RAM analysis by abstractly characterizing the life cycle, interactions, and externals of the system in question. Figure 6 presents a simplified context model for describing the surrounding elements (ie, blocks with gray) of USMs (ie, the block with black) and associated operational description and interface, in order to share this core concept agreed by various stakeholders.

The major need from stakeholders is to ensure the accuracy of USM readings against potential deterioration and expected variations from externals. The functional requirements can be elicited by analyzing the interfaces in Figure 6. For instance, factors related to the reading and calculation of USMs are setting of flow computers, readings of PT and TT and on-site master prover. In addition, environmental conditions on metering site (eg, ambient temperature and pressure, humidity), piping arrangement and thickness, and power and signal interfaces with electronic units, all can impact the performance of USMs. These functional requirements result in upgrading or detailing the existing design concept. For instance, the uninterrupted power unit may be needed by the flow computer to avoid possible power outages that cause the loss of data. The Norwegian measurement regulation requires the uncertainty to be less than 0.3% of standard volume. Given the analysis of current laboratory result, the uncertainty of this design concept is estimated to be less than 0.2% of standard volume at 95% confidence level.[44]

Based on Figure 6, it is assumed that each functional channel that fulfills the operational needs requires the signal interfaces between USM and SEU. There are two alternatives for configuration: configuration 1 is that all three USMs are connected to two SEUs, and configuration 2 is that one USM is connected to SEU and other two are connected to another SEU. This said, when there is a failure on a SEU connected to two USMs, the whole metering station loses two signal inputs from the USM assembly. Configuration 1 clearly offers higher operational flexibility as the SEU is fully redundant for each USM, at the same time introducing more complexity to the system due to the increasing number of jumpers. The failure of jumpers can cause jammed, interrupted, or missing signals, which can immediately cause an increase of measurement uncertainty and the need for maintenance. The maintenance of USM assembly includes several tasks such as full isolation of the metering station from the pipeline, removal of hydrocarbon in the units of metering station and lift of whole metering station through the rig. The length of downtime related to maintenance activities of USM assembly is assumed as 2 months (ie, 1440 hours). The faulty SEU and jumpers (ie, flexible connection between units) can be restored in 1 week (ie, 168 hours) after two signals from USM are lost.

Considering the expensive retrieval and intervention, the maintenance requirement agreed by stakeholders is that retrieval for calibration and adjustment is not required during the lifetime of the system (ie, 20 years). Consequently, a degraded performance of the flow metering module may be acceptable, which means operator may not immediately shutdown the flow metering module if two out of three USM outputs are lost. Assuming that uncertainty contributions from each USM are uncorrelated, the resulting measurement uncertainty approximately equals the reciprocal of the square root of the number of meters. For instance, if the measurement uncertainty is estimated as 0.15% for a single USM, the resulting uncertainty for two and three USMs are 0.11% and 0.09%, respectively.

To compare various maintenance strategies for USM assembly, the three possible maintenance strategies are as follows given the considerations from system designer:

- Strategy I: The activities related to maintenance starts immediately when two USM functions are affected, the metering station is shut down during maintenance.
- Strategy II: The activities related to maintenance postpone 1 year (ie, 8760 hours) when two USM functions are affected, the metering station is shut down during maintenance.
- Strategy III: The activities related to maintenance starts immediately when two USM functions are affected. At the end of lifetime

(ie, the last 5 years before intervention), it is acceptable to operate metering station with only one USM.

The three maintenance strategies imply different RAM performances for the given design concept. The insights to maintenance management had not been discussed in the prior versions of the design proposal from Statoil,[44] as it required participation of RAM analysts to build up a RAM model to simulate system responses under different maintenance strategies. This work requires the design analysis to study the system behavior for different configurations and under different maintenance strategies, which is elaborated in Subsection 5.3.

Considering two possible configurations and three different maintenance strategies, there are six cases in total for evaluation. The selection of design concept should consider the maintenance and spare parts costs related to the revealed failure modes and the risk for loss of profit and income related to measurement uncertainty, where all the losses are converted into a monetary unit, that is, Norwegian kroner (NOK). The result is briefly discussed in Subsection 5.5.

5.3 | Design analysis

Figure 7 presents different phases (retrieval, normal operation) in the life cycle of USM assembly and associated state transitions. In Figure 7, transitions including *component failure of USM*, *prepare for retrieval*, *shutdown and retrieval*, and *restoration* receive the main focus. The system is initially in the working state, where the measurement uncertainty is 0.09%. When one USM is lost, the system reaches minor degradation state and the measurement uncertainty is increased to 0.11%. When two USMs are lost, the system reaches the major degradation state and the measurement uncertainty is increased to 0.15%. When the system reaches this state, the maintenance event may be planned immediately (strategy I), or postponed with acceptance to operate under severe degradation (strategy II), or ignored, when in the later phase of operation (strategy III). This said, the condition for transition "*prepare for retrieval*" varies based on maintenance strategies. When all USMs are lost, the system must shutdown and prepare for maintenance immediately. After maintenance, the faulty USM are replaced (ie, as good as new) and metering station is restored to working operation state. The state diagrams for SEUs and jumpers can be established in the similar fashion. The functional dependencies between SEU, jumper, and USM can be established by synchronizing the transitions, see details in Subsection 5.4.

The state diagram clarifies the possible events, system states and associated transitions, which helps RAM analysts to correctly define the relevant modeling elements, that is, the required actors of normal operation and maintenance and conditions for retrieval processes. The functional dependences can be highlighted by employing such state space modeling, which is beyond the traditional analysis for hierarchy based analytical reduction such as functional trees or physical breakdowns. It may be noted that state-diagram is one of many methods to complete design analysis. The same information can be obtained using flow-based diagrams such as FFBD and activity diagrams.

The architectural aspects are obtained through design analysis in order to provide insight on the causes and consequence of hazards and the suitability of associated countermeasures. The physical attributes (eg, dimensions, materials, component quality, manufacture process, and locations) may impact system behavior. For instance, the location of metering should be distant from control valves, as the noise of valve operation can interfere with USM measurement. The identification of architecture for given system concept assists in following RAM analysis, especially for dysfunctional analysis as shown in Subsection 5.4.

5.4 | RAM analysis

RAM analysis starts with dysfunctional analysis as indicated in Figure 4. Here, FMECA is selected as hazard identification methods, and the part of the FMECA are presented in Table 3. The failure rate for each failure mode is shown in the last column of Table 3, which is estimated based on the original data provided in the recognized database for subsea application OREDA[45] together with expert judgments about influencing factors for each failure mode. The reader interested in a detailed specification for criteria for selecting influencing factors and procedures for failure rate estimation can refer to Brissaud et al.[46,47] In this case study, only critical failures that lead to the loss of performance are taken into account, where the incipient failures or degradation are removed from scope.

With the information in Table 3 and the system concept developed in design analysis, it is possible to construct a RAM model. The general assumptions and constraints are made on the basis of both design analysis and operational analysis as follows, and they are valid for all cases to be evaluated:

- For each USM, SEU and jumper only consider two states: faulty and working.
- The sensor lines are continuously checked, thus the delay for detecting failures on jumper and SEU can be ignored.
- All components are considered as good as new after maintenance. The activities of maintenance are considered as perfect, thus no adverse effects are induced.
- Ideally, the subsea operator does not expect any retrieval during the operation until the metering system cannot perform the function as intended. Assuming that restoration duration $\omega = 8$ hours and mobilization time $\eta = 1440$ hours (ie, 2 months), and the intervention will be carried out after 20 years of installation (ie, 175 200 hours).

There are many suitable approaches for the following quantitative analysis, for example, Petri nets. Figure 8 presents partial Petri nets for case 1 (ie, configuration 1 following strategy I), where state-transitions in Figure 7 are mapping into Figure 8 by the *predicates* and *assertions* in the Petri nets. Predicate (represented by "?") is a formula to validate the transitions, and assertion (often represented by "!") is a formula to update the variables after the associated transition is fired.[48] The instruction for constructing Petri nets model can be found in articles of Signoret et al[48] and Signoret.[49] The synchronization of transitions indicates how each USM input is considered as valid or invalid given the states of USMs, jumpers, and SEUs. The number of valid USM input is used to determine when to start maintenance and the uncertainty increment. For instance, case 1 follows maintenance strategy I

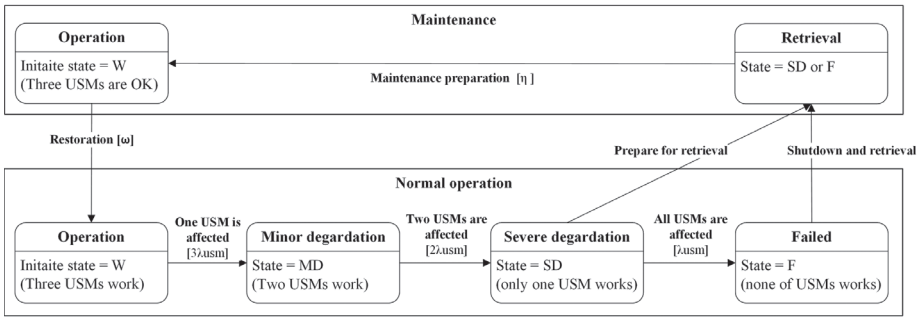
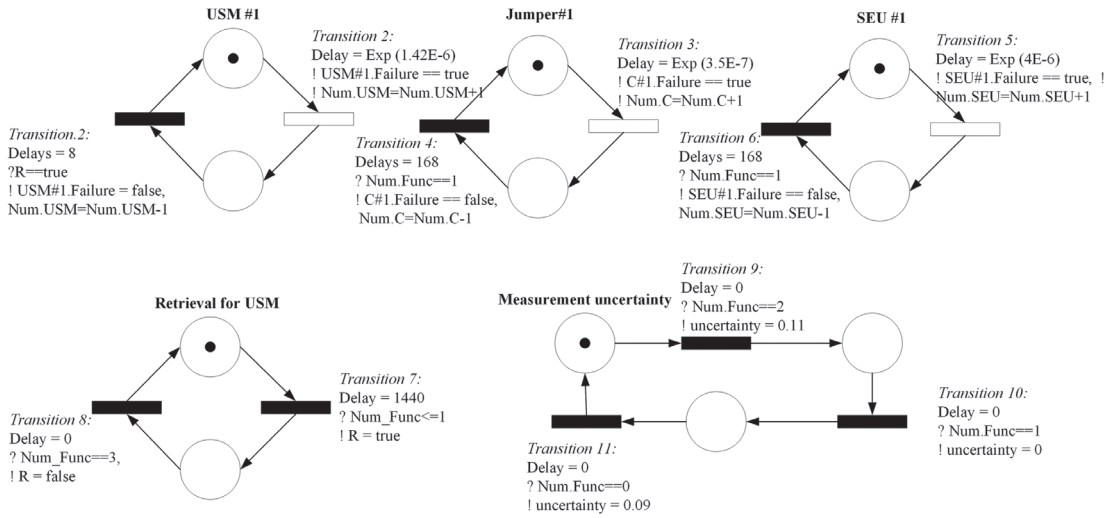


FIGURE 7 State diagram for USM assembly

TABLE 3 Selected results for qualitative RAM analysis

Unit	Failure mode	Failure mechanism	Failure rate (per 10^6 hours)
USM	Abnormal instrument reading	Changes in flow profiles, ultrasonic noise, high velocity (eg, turbulence)	0.82
	Erratic output	Transducer failure, instrument or material failure	0.6
Jumper	Lose of connection	Water intrusion or loss of resistance	0.35
SEU	Control failure	Flawed control algorithm (fault signal/alarm), leakage, software failure	3
	Other types	–	1.05



Synchronization of transitions:
Func.1= 1 if USM1 is working and either jumper1 and jumper2 is working and either SEU1 and SEU2 is working, else 0
Func.2= 1 if USM2 is working and either jumper1 and jumper2 is working and either SEU1 and SEU2 is working, else 0
Func.3= 1 if USM3 is working and either jumper1 and jumper2 is working and either SEU1 and SEU2 is working, else 0
Num.Func=Func.1+Func.2+Func.3

FIGURE 8 Petri nets model for case 1

and then the maintenance of USM assembly is planned when two valid USM inputs are lost. Petri nets model of cases 2-6 are constructed in the same way.

The computation for RAM modeling is completed by the software GRaphical Interface for reliability Forecasting.[50] The simulation run is set to be 100 000 to get the result with confidence. The downtime and retrieval frequency of cases 1-6 is reported in Table 4 and measurement uncertainty of cases 1-6 is illustrated in Figure 9. From Figure 9 and Table 4, one may notice the following points:

- The downtime reported in Table 4 not only considers the retrieval frequency of USM assembly but also the downtime to replace

TABLE 4 Downtime and retrieval frequency for cases 1-6

Case number	Expected downtime (hours)	Expected retrieval frequency
1. (Configuration 1, strategy I)	249	0.1733
2. (Configuration 1, strategy II)	225	0.1563
3. (Configuration 1, strategy III)	157	0.1092
4. (Configuration 2, strategy I)	418	0.2127
5. (Configuration 2, strategy II)	402	0.1988
6. (Configuration 2, strategy III)	391	0.1923

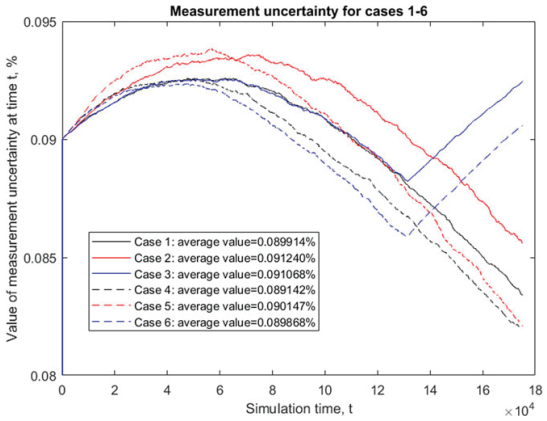


FIGURE 9 Measurement uncertainty for cases 1-6

jumper and SEU. As a result, configuration 2 (cases 4-6) has much more downtime than configuration 1 (cases 1-3).

- Applying strategy II (cases 2 and 5) needs less maintenance than applying strategy I (cases 1 4) by paying the price of allowing an increase in measurement uncertainty.
- Applying strategy III (cases 3 and 6) results in the increment of measurement uncertainty in the last 5 years of lifetime (ie, the turning points in Figure 9) as the system is allowed to operate with single USM. The downtime due to maintenance is significantly reduced compared to strategies I and II for configuration 1 (cases 1 and 2), however, not for configuration 2 (cases 4 and 5).
- Configuration 2 (cases 4-6) has more maintenance needs than configuration 1 (cases 1-3), and the maintenance need does not vary too much given the different maintenance strategies. As result, the measurement uncertainty is decreased.
- The peak value of measurement uncertainty for configuration 2 (cases 4-6) comes earlier than configuration 1 (cases 1-3). The reason is that configuration 2 loses flexibility as the SEU is not fully redundant for each USM.

5.5 | Joint concept analysis and communication

The objective of joint concept analysis is to present some common themes that cannot be solved or considered by any individual engineering discipline. Table 5 presents some major considerations derived from the selected analysis in RAM-SE framework. These considerations may either require designers to reevaluate the system concept, or RAM analysts to reconstruct the RAM model to achieve more realistic design implications. For example, the maintainability analysis shows that it is necessary to consider the separation between measurement instruments and sampling systems. Therefore, DSM is required for design analysis for mastering the interaction between these two modules and subsequent RAM analysis. Another example could be CCF assessment. The series connection of duty USM, master USM, and spare USM can introduce the common mode errors due to the same design, installation, and function. In this case study, common failure mode for USMs is mainly the deposits, for example, wax. The designer indicated that the implemented measure is to heat the flow, thus prevent wax formation.[44] Such communication should be documented and registered. If the related measure cannot be implemented given other design constraints (eg, space and cost for heating strategy), then the effect of CCF should be incorporated in the calculation and modeling and the RAM model in Figure 8 will be updated to introduce the associated events.

The constraint-based decision making, such as lifecycle cost analysis, should be used to select the cost-effective alternatives for this design concept. The result of previous RAM analysis gives indications for two cost functions in lifecycle analysis: the total cost for maintenance including resource mobilization and spare parts, and the profit loss due to system downtime and measurement uncertainty. The selection criteria for costs functions and procedure of cost analysis can follow the existing standards such as NORSOK I-106[51] or the internal procedure of the oil company. For instance, in this case study, the net present value of oil in subsea storage is assumed as 200 billion NOK and direct costs to replace the USM assembly is estimated as 25 million NOK. The result of cost analysis shows that case 1 saves the most. Compared to the most costly case 2, case 1 can save 4.03 million NOK in stakeholder's favor during the operation of 20 years, without considering the purchase order cost, project costs, and technology development costs.

Communication plays an essential role in any engineering process as illustrated in the RAM-SE framework. What is meant by communication here is not documenting the numerical results that may fall into "playing a number game" but *telling the story* based on a consistent background. In this case study, by performing operational analysis and design analysis, RAM analysts can easily identify what is beyond the normal operations viewpoint and clarify the assumptions and simplifications for RAM modeling. The result of RAM modeling is thereby

TABLE 5 Considerations for USM design

Analysis	Key results and comments	Updated design constraints or required follow-up analysis
Zonal analysis[3]	• The noise of control valves can influence USM performance. • PT installed in the close location may cause the turbulences that influence USM performance.	• Develops strategy and associated equipment to reduce the effect of noise if cost and space allows, for example, noise trap or bends in piping. • Keep the necessary distance between PT and USM, for example, at least three diameters of downstream.[54]
CCF assessment	• The series connection of USM offers better quality monitoring capacities but common mode errors of USM are introduced, which can influence the performance of USM and calibration process.	• Develops strategy for eliminating the potential factors on CCF, for example, improve manufacturing process and upgrade on-site calibration process by taking CCF into account, see also the guideline in IEC61508.[55] If not, CCF must be incorporated in relevant RAM modeling.
Maintainability analysis[53]	• The sampling system has higher maintenance needs than metering module.	• The sampling system can be in a separate module to offer better RAM performance if cost and space allows.

situated in a well-defined context to support the decision making in a design process. In this case study, by starting with operational analysis, the issue to be investigated is specified: the impact of maintenance strategies and configurations. Design analysis identifies the functional and architectural aspects behind the issue: the system behavior (ie, states and transitions) of selected configurations under different maintenance strategies. The information can be used to construct a RAM model and the numerical results through simulation can be used for selection of design alternatives. It is important to remember that the using RAM-SE framework is never to prove that models are close to the reality but to ensure RAM analysis are illuminating and useful to consider the design implications when the context is defined properly.

6 | CONCLUSION

It has become apparent that incorporating RAMS aspects as early as possible gives several advantages in form of engineering efforts and budgets. Many companies involved in subsea development have their procedures for framing RAM in design but they still claim that they are not adequate. The similar problem already exists in many industry sectors such as nuclear, satellite, and aviation, where the problem is further amplified by the complexity of design solutions. This article selects subsea design as the starting point. Analysts in this context, often dive into RAM analysis before correctly stating the system concept. Development of a system concept by RAM techniques relies on competence, experience, and the knowledge base of analysts, which often results in inconsistency and misunderstandings. Without a more holistic framing, RAM in subsea design has limited possibility to give systematic insight of the design concept, making it necessary to integrate other disciplines to complete industry practice.

This article discloses the link between the RAM discipline and SE. Through the analysis, the authors propose a RAM-SE framework to connect the concepts and models used by these two disciplines, in light of specific issues encountered in subsea design. The framework identifies the benefits that RAM engineers appreciate the SE methods that can support RAM and vice versa. Analysis based on the SE suite of tools could be a prerequisite for specialty analysis like RAM analysis to reduce the risk of working from an inconsistent and incorrect system concept. Then, system designers can correctly capture the indications derived from RAM analysis conducted in a systematic and iterative manner. The case study demonstrates how the new subsea design was evaluated from different point of interests using the RAM-SE framework. Although the selected case is quite restrictive and simple, it can be used to illustrate the challenges encountered when framing RAM aspects of subsea design, such as functional/physical interactions that can result in complex maintenance and test strategies.

This framework serves as a baseline for further refinement in order to direct future effort to improve the process of framing RAM in subsea design. The process described by the RAM-SE framework is highly simplified and idealized. First, RAM-SE framework only restrictively discusses interlinks between these two disciplines in light of models with high acceptance and commonality in each community, for example, SysML. This said, the design analysis and RAM analysis are conducted in sequence thus some overlaps may be latent as system theory or system thinking is indirectly placed in conducting RAM analysis. Additional research could develop RAM methods directly using system theory. One such pioneer work has been completed by Leveson[15] who use system theory to create a new accident model used for safety analysis. However, similar work has not been found in RAM domain yet. Moreover, the application is here only demonstrated within subsea design. One remaining work of this article can be to expand the analysis to consider other sectors to enrich the content of the proposed framework and hopefully bring ideas for transfer of knowledge from this article to other domains of interest. Our suggestion for improving this framework is to further test the proposal against an industry-size case.

ACKNOWLEDGMENTS

This work was carried out as a part of Subsea Production and Processing (SUBPRO), a research-based innovation center within SUBPRO. The authors gratefully acknowledge the project support, which is financed by the Research Council of Norway, major industry partners and NTNU. Special thanks to our colleague, Antoine Rauzy, who continuously contributes to this body of knowledge and provides inspirations on current issues facing both the RAM and SE communities. The authors are also grateful for the valuable comments and useful suggestions of two anonymous reviewers.

ORCID

Juntao Zhang http://orcid.org/0000-0001-9972-2078
Cecilia Haskins http://orcid.org/0000-0002-2506-8808
Yiliu Liu http://orcid.org/0000-0002-0612-2231
Mary Ann Lundteigen http://orcid.org/0000-0002-9045-6815

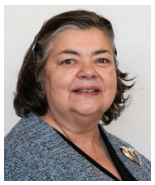
REFERENCES

1. Stapelberg RF. *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*. London, England: Springer; 2009.
2. ISO 26262. *Road Vehicles—Functional Safety*. Geneva, Switzerland: International Organization for Standardization; 2011.
3. SAE ARP4761. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Warrendale, PA: Society of Automotive Engineers; 1996.
4. IEC 61513. *Nuclear Power Plants—Instrumentation and Control Important to Safety—General Requirements for Systems*. London, England: British Standards Institution; 2011.
5. ISO 20815. *Petroleum, Petrochemical and Natural Gas Industries–Production Assurance and Reliability Management*. Geneva, Switzerland: International Organization for Standardization; 2008.
6. EN50126. *Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. London, England: British Standards Institution; 1999.
7. INCOSE. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, Version 4.0*. Hoboken, NJ: John Wiley and Sons; 2015.
8. SUBPRO. *Subsea production and processing*. 2015. https://www.ntnu.edu/subpro. Accessed February 16, 2018.
9. Kusiak A. *Concurrent Engineering: Automation, Tools, and Techniques*. Hoboken, NJ: John Wiley and Sons; 1993.
10. Crowe D, Feinberg A. *Design for Reliability*. Boca Raton, FL: CRC Press; 2001.
11. Mettas A. Design for reliability: overview of the process and applicable techniques. *Int J Perform Eng*. 2010;6:577–586.
12. INCOSE. *Systems Engineering*; 2001 https://www.incose.org/systems-engineering. Accessed July 06, 2018.
13. Jigar AA, Haskins C, Lundteigen MA. Availability allocation using systems engineering principles. Paper presented at: International Conference on Industrial Engineering and Operations Management; 2016; Kuala Lumpur, Malaysia.
14. Garro A, Tundis A. On the reliability analysis of systems and SoS: the RAMSAS method and related extensions. *IEEE Syst J*. 2015;9(1):232–241.
15. Leveson N. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press; 2011.
16. Ramberg RM, Davies SR, Rognoe H, Oekland O. *Steps to the Subsea Factory*. Paper presented at: Offshore Technology Conference; 2013, Rio de Janeiro, Brazil.
17. DNV-RP-A203. *Qualification of New Technology*. Høvik, Norway: DNV; 2011.
18. API-RP-17N. *Recommended Practice Subsea Production System Reliability and Technical Risk Management*. Washington, DC: American Petroleum Institute; 2009.
19. O'Connor P, Kleyner A. *Practical Reliability Engineering*. 5th ed. Hoboken, NJ: John Wiley and Sons; 2012.
20. Verma AK, Ajit S, Karanki DR. *Reliability and Safety Engineering*. London, England: Springer London Ltd.; 2015.
21. Bertsche B. *Reliability in Automotive and Mechanical Engineering*. Berlin, Germany: Springer; 2008.
22. Johansson C. *On System Safety and Reliability Methods in Early Design Phases* [PhD thesis]. Linköping, Sweden: Department of Management and Engineering, Linköping University; 2013.
23. Johansen IL, Rausand M. Defining complexity for risk assessment of sociotechnical systems: a conceptual framework. *Proc Inst Mech Eng O*. 2014;228(3):272–290.
24. Barnard RWA. What is wrong with reliability engineering? Paper presented at: Proceedings of the 18th Annual INCOSE International Symposium; 2008; Utrecht, The Netherlands.
25. IEC 60812. *Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA)*. Geneva, Switzerland: International Electrotechnical Commission; 2006.
26. Stamatis DH. *Failure Mode and Effect Analysis—FMEA from Theory to Execution*. 2nd ed. Milwaukee, WI: ASQ Quality Press; 2003.
27. Blanchard BS, Fabrycky WJ. *Systems Engineering and Analysis*. Upper Saddle River, NJ: Prentice-Hall; 1998.
28. Asbjørnsen O. *Systems Engineering Principles and Practices*. Norwood, MA: Skarpodd; 1992.
29. Haskins C. *Systems engineering analyzed, synthesized, and applied to sustainable industrial park development*. Tapir Akademisk Forlag 2008:175 (ISBN 978-82-471-1028-7) 141 pages; 2008.
30. Dahl HJ. Information modelling and systems re-engineering: An efficient approach to assessing complex current Norwegian natural gas transport operation. Paper presented at: Proceedings of Tenth Annual International Symposium on the International Council on Systems Engineering (INCOSE); 2000; Minneapolis, MN.
31. Dahl HJ. *Norwegian Natural Gas Transportation Systems. Operations in a Liberalized European Gas Market* [Ph.D. thesis]. Trondheim, Norway: NTNU; 2001.
32. Long D, Scott Z. *A Primer for Model-Based Systems Engineering*. Blacksburg, VA: Vitech Corporation; 2012.
33. OMG. OMG Systems Modeling Language (SysML). http://www.omg.org/index.htm. 2017. Accessed November 07, 2018.
34. Clarkson M. A stakeholder framework for evaluating corporate social performance. *Acad Manag Rev*. 1996;20. http://doi.org/10.2307/258888.
35. Friedenthal S, Moore A, Steiner R. *A Practical Guide to SysML*. 3rd ed. Boston, MA: Morgan Kaufmann; 2015.
36. IEC 60300 3–4. *Dependability Management—Guide to the Specification of Dependability Requirements*. London, England: British Standards Institution; 2007.
37. Eshuis R, Wieringa R. Comparing Petri net and activity diagram variants for workflow modelling: a quest for reactive Petri nets. *Petri Net Technol Commun Based Syst LNCS*. 2003;2472:321–351.
38. Yang N, Yu H, Sun H, Qian Z. Mapping UML activity diagrams to analyzable Petri net models. Paper presented at: 2010 10th International Conference on Quality Software; 2010; Zhangjiajie, China.
39. Andrade E, Maciel P, Callou G, Nogueira B. A methodology for mapping SysML activity diagram to time Petri net for requirement validation of embedded real-time systems with energy constraints. Paper presented at: 2009 3rd International Conference on Digital Society; 2009; Athens, Greece.
40. NASA. *NASA Systems Engineering Handbook*. Washington, DC: National Aeronautics and Space Administration; 2007
41. Eppinger SD, Browning TR. *Design Structure Matrix Methods and Applications*. Cambridge, MA: MIT Press; 2012.

42. Ryan J, Sarkani S, Mazzuchi T. Leveraging variability modeling techniques for architecture trade studies and analysis. *Syst Eng*. 2014;17(1):10–25.
43. Daniels J, Werner PW, Bahill AT. Quantitative methods for tradeoff analyses. *Syst Eng*. 2001;4(3):190–212.
44. Statoil. *Design of a subsea fiscal oil export metering system*. Paper presented at: NSFMW 2015; 2015; Tønsberg, Norway.
45. OREDA. *Offshore and Onshore Reliability Data*. 6th ed. Norway: OREDA Participants; 2015.
46. Brissaud F, Charpentier D, Fouladirad M, Barros A, Bérenguer C. Failure rate evaluation with influencing factors. *J Loss Prev Process Ind*. 2010;23:187–193.
47. Brissaud F, Barros A, Bérenguer C, Charpentier D. Reliability analysis for new technology-based transmitters. *Reliab Eng Syst Saf*. 2011;96:299–313.
48. Signoret J-P, Dutuit Y, Cacheux P-J, Folleau C, Collas S, Thomas P. Make your Petri nets understandable: reliability block diagrams driven Petri nets. *Reliab Eng Syst Saf*. 2013;113:61–75.
49. Signoret J-P. Dependability and safety modeling and calculation: Petri nets. Paper presented at: Proceeding of the 2nd IFAC Workshop on Dependable Control of Descrete Systems; 2009; Bari, Italy.
50. GRIF. *Graphical Interface for Reliability Forecasting*. France: SATODEV (company); 2016.
51. NORSOK I-106. *Fiscal Metering Systems for Hydrocarbon Liquid and Gas*. Norway: Norsk Sokkels Konkuranseposisjon; 2014.
52. Issad M, Kloul L, Rauzy A. *A scenario-based FMEA method and its evaluation in a railway context*. Paper presented at: Reliability and Maintainability Symposium (RAMS); Orlando, Florida, USA 2017.
53. IEC 60300-3-10. *Dependability management-Part 3–10: Application Guide Maintainability*. Geneva, Switzerland: International Electrotechnical Commission; 2001
54. AGA-Report No. 9. *Measurement of Gas by Multipath Ultrasonic Meters*. Arlington, Virginia, USA: American Gas Association; 1998.
55. IEC 61508. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*. Parts 1–7. Geneva, Switzerland: International Electrotechnical Commission; 2010.
56. Ramírez PAP, Utne IB, Haskins C. Application of systems engineering to integrate ageing management into maintenance management of oil and gas facilities. *Syst Eng*. 2013;16:329–345.
57. Shainee M, Haskins C, Ellingsen H, Leira BJ. Designing offshore fish cages using systems engineering principles. *Syst Eng*. 2012;15:396–406.

AUTHORS' BIOGRAPHIES

Juntao Zhang is a Ph.D. candidate in the Reliability, Availability, Maintainability and Safety Programme in the Department of Mechanical and Industrial Engineering, at the Norwegian University of Science and Technology (NTNU). He earned a bachelor degree from Electromechanical Engineering Department at the University of Macau, Taipa, Macau, and a master degree from Department of Mechanical and Industrial Engineering, NTNU, Trondheim, Norway. With the help of the blend of technical and managerial perspectives from the education background, He is currently working on the reliability project in the 8-year research centre on subsea production and processing (SUBPRO). His research interest is in the area of incorporating reliability and availability in the early phase of subsea design process.



Cecilia Haskins is an American living and working in Norway and blending the best of both cultures into her personal and professional life. Her educational background includes a BSc in Chemistry from Chestnut Hill College, Philadelphia, PA, and an MBA from Wharton, University of Pennsylvania, Philadelphia. She has been recognized as a Certified Systems Engineering Professional since 2004. After earning her Ph.D. in Systems Engineering from the Norwegian University of Science and Technology (NTNU), Trondheim, Norway, she has conducted postdoctoral research on innovative applications of systems engineering to sociotechnical problems such as those encountered in sustainable development and global production systems.

Yiliu Liu has been an associate professor in the Department of Production and Quality Engineering, Norwegian University of Science and Technology (NTNU) since the beginning of 2013. Before that, he had worked as a post doctor fellow in the same department from 2011 to 2012. His main research interests include system reliability and resilience engineering, safety critical systems and risk management. Dr Liu is very active now in the relevant fields, with publishing 3 book chapters and more than 60 peer-reviewed papers (28 on international journals). Most of the publications appear in the recent 5 years. He is also serving the academics as the reviewer for more than 20 international journals and the technical committee member for more than 10 international conferences. Dr. Liu is the coordinator and main lecturer for two master courses in NTNU, and he also serves as the director of the international master program of RAMS (reliability, availability, maintainability and safety). He has deeply involved in several research projects funded by Norwegian research council, NTNU and other institutions. In addition, Dr. Liu has a robust research network with universities in different 10 countries.

Mary Ann Lundteigen has been a professor in Department of Mechanical and Industrial Engineering since 2011, with a period with DNV-GL as Principle Engineer from 2012-2013. She has a PhD in reliability of safety-instrumented systems (2009), and a MSc. in engineering cybernetics (1993). Before starting on her PhD, she worked for several years in industry, including as instrumentation engineer (onshore) and automation and electrical supervisor (offshore) in Phillips Petroleum, automation leader at the factory of Nidar, and senior researcher at SINTEF, department for applied cybernetics. Her main research focus and interest concern functional safety and reliability of safety-related electrical/electronic/programmable electronic (E/E/PE) systems. She is also a member of IEC 61511 committee who maintains

the standard on functional safety for process industry sector. As a co-director and responsible for reliability subject in the 8-year research centre on subsea production and processing (SUBPRO, see http://www.ntnu.edu/subpro), she has extended her research to cover reliability, safety, and condition-based maintenance of systems with particular demanding environmental and operational conditions, such as subsea systems. Lundteigen has a long-lasting and extensive contact network in Norwegian industry work, due to involvement in SINTEF projects over several years, many of the m through the PDS forum (http://www.sintef.edu/pds). She has more than 50 publications peer-reviewed papers, including around 20 papers in international journals. She has also been contributing to a high number of studies for industry companies.

How to cite this article: Zhang J, Haskins C, Liu Y, Lundteigen MA. A systems engineering–based approach for framing reliability, availability, and maintainability: A case study for subsea design. *Systems Engineering*. 2018;1–17. https://doi.org/10.1002/sys.21462

Combining System-Theoretic Process Analysis and availability assessment: a subsea case study

Zhang J, Kim H, Liu Y, Lundteigen MA. Combining System-Theoretic Process Analysis and availability assessment: a subsea case study. *Revised Manuscript under review in*; *Proceedings of Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*. 2018

Combining System-Theoretic Process Analysis and availability assessment: a subsea case study

Juntao Zhang[1], HyungJu Kim[1], Yiliu Liu[1], Mary Ann Lundteigen[1]

[1]Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, Trondheim, Norway

Abstract: Hazard identification methods are important tools to verify that the system is able to operate according to specifications under different operating conditions. Unfortunately, many of the traditional methods are not adequate to capture possible dysfunctional behavior of complex systems that involve highly coupled parts, non-linear interactions and software-intensive functionalities. The rather recent method named System-Theoretic Process Analysis (STPA) is one promising candidate to improve the coverage of hazard identification in complex and software-intensive system. Still, there is no guideline for utilizing STPA output to evaluate the potential of loss, which is important for basis for decision-making about system configuration and equipment selection. The focus of this article is placing on the interface between STPA and reliability, availability and maintainability (RAM) analysis. The approach named STPA-RAM model is proposed to translate feedback control loops into Stochastic Petri-nets for discrete event simulation. The proposed approach is demonstrated with a simple case related to subsea design concept. The major conclusion is that STPA-RAM model extends the application of STPA, while also improving, and as such reducing completeness uncertainty and model uncertainty, associated with input data and information for RAM analysis.

Keyword: Reliability, Systematic approach, Complexity, Subsea system

1. INTRODUCTION

Highly coupled parts, non-linear interactions and software-intensive functionalities characterize modern engineering systems. One example could be subsea systems for Oil and Gas (O&G) production and processing. Traditional technologies for subsea control (e.g. hydraulically operated systems) have been gradually replaced by computer-based technology to fulfill the needs of higher level of autonomy, self-diagnostics and monitoring. Such a shift in technologies gives opportunities for more cost-efficient and autonomous operation in marginal subsea fields that have special restrictions associated with accessibility [1]. In this respect, understanding hazards caused by complex interactions on software-intensive systems becomes an important topic. This topic involves two critical steps: the first is to reveal the potential hazards for given design concept, namely hazard identification; the second is to quantify the consequence of critical hazards, to direct engineering efforts to improve reliability, availability and maintainability (RAM) performance.

Subsea control systems include sensors, actuators and controller that interact with the controlled process and other connected systems, such as systems on-board an offshore platform or onshore at the receiving facilities. Loss of critical functionality is not only the result of component faults but also the improper interactions when components are brought together, i.e. the technologies interact in response to the internal and external environment. Unfortunately, identifying hazards arisen from improper interactions is beyond the scope of traditional methods, such as Failure Mode, Effects and Criticality Analysis (FMECA) and Hazard and Operability study (HAZOP) [2, 3]. FMECA focuses on the failure modes and causes of distinct components, whilst HAZOP has a more focus on the consequences of deviations related to process parameters, software functions and procedures. In FMECA or HAZOP, components, process objects, or procedures are analyzed one by one and the interactions are analyzed pairwise. For complex and software-intensive systems, it is important to also complement with analyses that are able to identify failure modes and dysfunctional behavior beyond the physical failures. Some candidate solutions have been proposed by researchers, such as Accimap [4], blended hazard identification method (BLHAZID) [5], functional resonance analysis method (FRAM) [6] and Systems-Theoretic Process Analysis (STPA) [7]. Of the mentioned methods, STPA is the approach

attracting the most recent attention due to its suitability to analyze complex and software intensive systems. Some of the advantages and examples of applications of STPA are discussed in [8-10].

STPA is based on a rather new accident causation model named Systems Theoretic Accident Model and Processes (STAMP), which is built on a theoretical basis provided by system theory and control theory [2]. STPA identifies hazards in a systematic way by examining the potential deviations on the defined feedback control loop. A feedback control loop is a graphical representation, which involves all the actors that have impacts on the emergent system properties in form of their individual behavior and interactions. Each actor is identified by its responsibilities (e.g. tasks/commands) and its reliance on information/feedback. The improper or inadequate combination of control commands and feedbacks can result in loss of vital values, such as human losses, environmental losses, customer dissatisfaction and economic losses. STPA has been applied in different applications such as automotive [11], healthcare [12], aerospace [13], maritime [14] and subsea [9, 15]. As a hazard identification method, STPA can be naturally embedded in safety and security analysis [16, 17] by guiding the associated controls and mitigating measures depending on different applications [12, 18, 19]. So far, the commonality and acceptance of STPA are limited to the academic studies and not yet adapted as best practices in e.g. international standards on safety assessments. Yet, it seems very promising to use STPA as complementary to FMECA and HAZOP to efficiently increase the coverage of hazard identification thus reduce the potential of accidents [10].

STPA provides an alternative model to identify hazards of complex and software-intensive systems. Yet, STPA has no interface with RAM models thus it is not fully clear how to interpret STPA outputs in the decision context. RAM models characterize the combinations of evolutions (e.g. degradation and failure) and maintenances (e.g. replacement and repair), and is used to demonstrate a certain level of RAM performance before the new design concepts for systems are qualified for the intended use. Few attempts have been made to systematically use STPA outputs to improve RAM models, whereas a similar link can be readily found for traditional methods, e.g. FMECA and HAZOP. The lack of this connection is unfortunate as important insight can be overlooked and not transferred from STPA to RAM model. This is also pointed out by Hafver et al. [20], who suggest that the STPA output has the potential to construct better RAM model to predict the effect of improper/inadequate controls on system behavior.

With regard to the nature of modelling, RAM models can be classified as combinatorial approaches, or state-transition approaches that rely on event-chain description. Fault tree analysis (FTA) is one example of combinatorial approaches, where the occurrence or probability of loss is determined directly by the combination of events related to equipment failure and indirectly by the impact of human factors and external events [21]. Such a combinatorial approach holds strict assumption on independence between events, so it is only able to cover accident related to hardware that fails as a chain of event. The classical state-transition approaches are Markovian approach [22-24] and Stochastic Petri-nets (SPN) [25, 26], which prove to be more efficient in reflecting dynamics features of system behavior than combinatorial approach by paying the price of calculability [22, 27]. STPA has been able to identify dependencies with loss consequences beyond what is normally captured by FMECA and HAZOP. It is therefore of interest to investigate how STPA results can be utilized for constructing state-transition models. In this article, SPN is selected as it is theoretically more expressive than Markovian approach in terms of event synchronization and flow propagation [28]. From literature, some initial proposals to combine STPA with SPN have been found. They are mainly for qualitative analysis, for example to derive integrated hazard logs for safety-guided design [29] and to have formal models for conducting STPA [30]. Yet, adding quantitative analysis in STPA has not been fully exploited.

The main objective of this article is therefore to propose a new model named STPA-RAM to supplement qualitative STPA with quantification models using SPN. STPA is conducted to identify hazardous scenarios, by modelling system behavior into feedback control loops. The perturbation initiated on controller or controlled process can propagate into system-level losses if no constraint is enforced to invert the condition of having hazard. Considering the feedback control loop obtained in STPA is not an executable model, SPN is to model the coordination between the controlled process and controller, and simulate the system response under

specified variations of feedback control loop thus predict frequency of losses. An illustrative case study is carried out to demonstrate the application of proposed approach.

The following section 2 introduces original STPA succinctly and give some reflections about its applications. Section 3 proposes a step-wise approach for building STPA-RAM model, and describes how to structure feedback control loops into SPN. A conceptual subsea design is selected to illustrate the application of proposal in section 4. Finally, discussions and concluding remarks are presented in section 5.

2. STPA PROCEDURE AND APPLICATION

2.1 Overview of STPA procedure

The STPA approach has been under continuous development since emergence, and its framework can be complicated with respect to the analytical needs and constraints for practical use, e.g. [31]. This article follows the generic steps suggested in STPA handbook by Leveson and Thomas [7], which are illustrated in Figure 1:

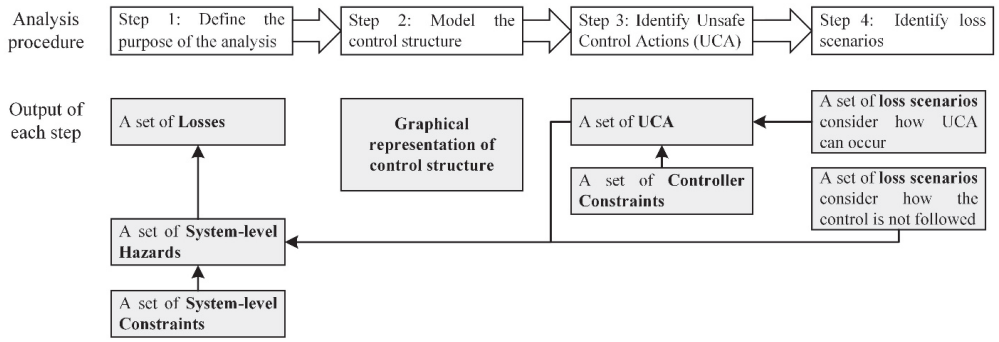


Figure 1 the framework of STPA and its output

- **Step 1: Define the purpose of analysis.** The first step is to define the scope of analysis by identifying the consequences on system level in presence of any single or multiple variations on feedback control loop. The consequence includes the losses and associated hazards. *Losses* could be any type of dissatisfactory value to stakeholder when the system fails to achieve its goal and objective, and system-level *hazards* are a set of system states that can lead to losses together with worst-case conditions. Such broad definition of losses and hazards implies that STPA covers traditional safety issues as well as RAM issues.
- **Step 2: Model the control structure.** The next step is to develop feedback control loops. The hierarchical control structure is composed into one or more feedback control loops, and visualize actors involved, control actions and feedback information. The objective is to have the global and complete vision about the hierarchy concern being controlled, thus supports the following step 3 and step 4. An example of a feedback control loop is illustrated in Figure 2, from the left to right the details are added based on the responsibilities assigned to each actor. The hierarchical control structure can be refined until the suitable granularity is reached.

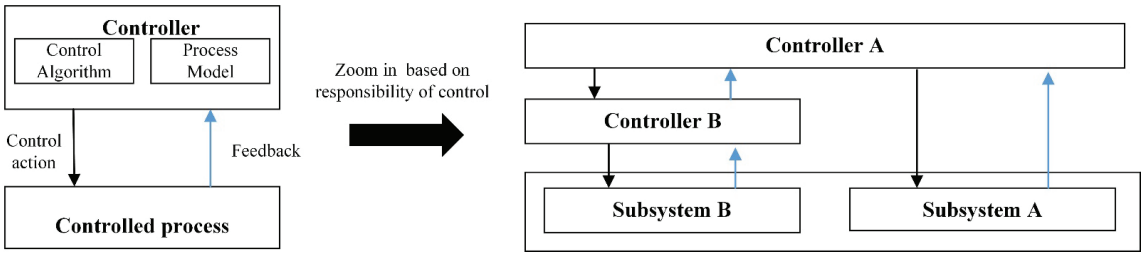


Figure 2 Example feedback control loop

- **Step 3: Identify Unsafe Control Actions (UCAs).** The third step relies on the structured identification of what can go wrong, using the feedback control loop and a prepared context table as basis. The output of this step is a list of UCA that in particular context results in one or more of the hazards identified in step 1. The UCAs are be identified through four guide conditions taking advantage of control structure: (1) the control action is not provided, (2) the unsafe control action is provided, (3) control action is provided too late, too early, or out of sequence and (4) control action is stopped too soon or applied too long (applied only for continuous control). The constraints for controller can be defined as conditions or behaviors to prevent occurrence of UCAs (and ultimately prevent related hazards).
- **Step 4: Identify loss scenarios.** Loss scenarios are used to describe the casual factors that lead to hazards (and ultimately to losses in worst-condition). The first type of loss scenarios consider how the UCA can occur, including the causes of unsafe controller behavior and inadequate feedback. The second type of loss scenario consider how the safe control action is not followed, including the causes of deviated control path and controlled process. The control structure obtained through step 2 need further refinement by including the sensors and actuator of the control loops so that analysts can examine why the feedback is not detected or wrongly detected and why the control action is not followed or improperly followed by actuators.

The new insight brought by STPA is the characterization of erroneous or inappropriate control and associated causality knowledge. All the possible contributions to the losses of a system (i.e. hardware, software, human and organizational factors) are considered as the elements (i.e. controller and controlled process) in the feedback control loop. The loss scenarios are determined when the *combination of* control commands, inadequate feedback, and the state of the controlled process and its environment is inadequate or improper. Such systematic way of hazard identification goes beyond the scope of traditional methods based on the common engineering sense (i.e. hardware-wise). In this respect, we argue that STPA is suitable for analyzing subsea system built today, which becomes increasingly intelligent and more dependent on software.

Whereas STPA theoretically increases the coverage of hazards, the current framework of STPA strictly emphasizes on qualitative aspects and has no guidance on how to direct the further quantification. In such set-up, STPA has no guidance on how to direct the further quantification of loss scenarios, which leaves designers with challenging tasks to interpret STPA results in the decision making. The architect of STPA, Leveson [2] has argued that quantitative analysis in STPA is questionable, for mainly two reasons. First, pursuing quantitative analysis can distract the attention away from important causal factors that are not characterized statistically [32]. Second, it requires probabilistic insights about future events that are not supported by historical data. Assigning probabilistic information for loss scenarios is a challenging and error-prone task even with excessive elaborations among system designers and experts.

Yet, there are also some reasons to extend STPA on a more quantitative basis. First, it is hardly possible to eliminate all possible loss scenarios in reality as countermeasures may degrade or become less efficient over time, see examples in [8, 19] where STPA is applied to technical system. It is therefore necessary to evaluate the effect of loss scenarios versus considerable costs for provision of countermeasures. Second, the lack of

data for probabilistic model does not mean the probabilistic model is useless in the context of STPA. The similar problem has been discussed by Bjerga et al. [33], who argued that rather than being pessimistic to discard probability, it is needed to advocate probabilistic analysis to address risks induced by potential systemic accidents, so that STPA results can be confidently used in a decision context.

In a short summary, we argue that current STPA framework has both advantages and inadequacies. Although STPA reveals a full spectrum of vulnerable points for given design concept, it leaves all judgments about prioritization of design improvements and modifications to the designers. The effect of designed countermeasures may not be obvious without constructing quantification model. Stimulating how the system responses to perturbations on feedback control loop through a defined mathematical framework can be a solution to this problem. That is the topic of next section.

2.2 Theoretical basis for simulation

According to Thomas [34], an UCA (and its descendant – loss scenarios) can be defined with a formal structure as a quadruple <***Ac***, ***CA***, ***Co, U***>, where:

- ***Ac*** is a set of actors refer to at least one controller of the controlled process.
- ***CA*** is a set of control commands issued by controller Ac ∈ ***Ac***.
- ***Co*** is a set of contexts that defines a unique system state, which implies whether the control action is needed (given) or not. ***Co*** can be specified explicitly or implicitly in terms of distinct variables. Each Co for the controller Ac should be independent.
- ***U*** is a set of hazardous state (i.e. description of possible and relevant losses). To be qualified as UCA, a control action must satisfy the property that (Ac, CA, Co) can lead to at least one of U ∈ ***U***

A control process can be equivalently transferred into Finite State Automata (FSA). FSA is used to model the discrete behavior of system, consists of a finite number of state, transitions between states and events. The *state* represents a quiescent node in the sequence of a control process, and the *event* describes the control action to be performed. A control-like *transition* triggered by an event or condition can cause the change of state. For instance, if providing a control action under a specific context that causes hazards, the transition function is ***T***: ***Co*** × ***CA*** →***U***. In this sense, the system in question is reformulated as the closed-loop control where the feedback signals (i.e. state of system) are now being used to both control and adjust itself.

The change of states (i.e. ***Co***) is modelled by random and deterministic events defined for a system. RAM model is one example, in which the failure and degradation are considered as stochastic events and software updates and hardware replacement are considered as deterministic. Therefore, one can establish the interface between RAM model and loss scenarios derived by STPA through FSA. The effect of loss scenarios on RAM performance can be simulated by FSA under the following assumptions: The transitions between states describe the situation where the control actions (no matter safe or unsafe) update values of model parameters (e.g. failure rate) in the new state. The changes made for model parameters influence the related transitions in FSA as a function of time. For example, a shutdown valve may be exposed to the hard stress in the situation of 'slam shut' closure, which can be seen as a loss scenario and its consequence is the permanent damage on valve. This implies the accelerated degradation rate for the shutdown valve once reaching the hazardous state that defines above situation.

Given such settings, the next chapter presents the proposal for hazard quantification, named STPA-RAM model. SPN is selected as the suitable modelling approach that follows state-event transition formalism.

3. PROPOSAL: STPA-RAM MODEL

3.1 Two-step approach

Figure 3 illustrates the two-step approach: The first step is to carry out an STPA to identify loss scenarios. The second step has to main sub-tasks: (i) to prepare RAM model using available specifications for the system and its intended functions, and (ii) to complement this model with new information from STPA in the first step. The outcome is a revised RAM model representing new information about dependencies in the feedback control loop developed by the STPA, namely a STPA-RAM model.

In the approach, the STPA-RAM model can reflect the potential deviations in different feedback control loops and interfaces between feedback control loops. Causality knowledge obtained in STPA is maintained in the STPA-RAM model. The loss scenarios can be generated by studying the reachability to the hazardous states. The actors of feedback control loops (i.e. hardware, software and organizational factors including human) are closely tied together in FSA in which the interdependencies between feedback control loops are represented by transitions. To maintain in the same format for integration, RAM model is constructed as the feedback control loop. In this regard, the monitoring and inspection on the state of controlled process are the considered as the feedback loop to the maintenance and intervention controller, whose responsibility is to update the software or replace the hardware when the feedback indicates the malfunctions and deviations of controlled process. Such modelling approach goes beyond the classical RAM model that is built on propagating the information from low-level system hierarchy along with simple logics.

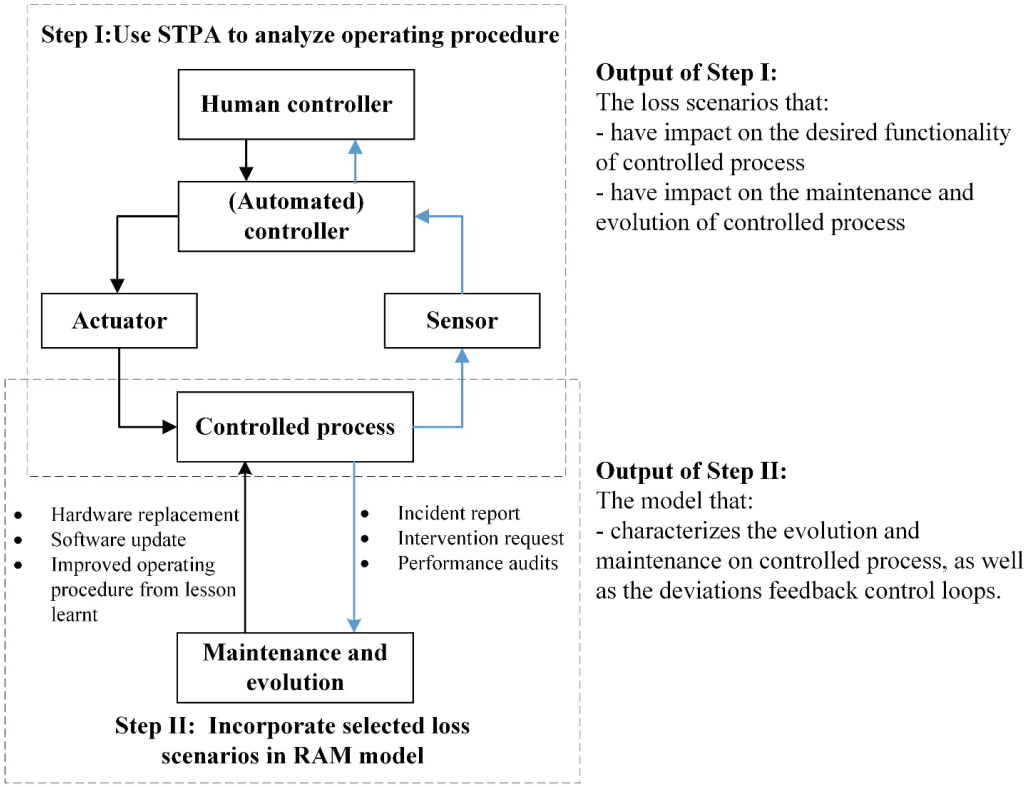


Figure 3 Two-step approach for STPA-RAM model

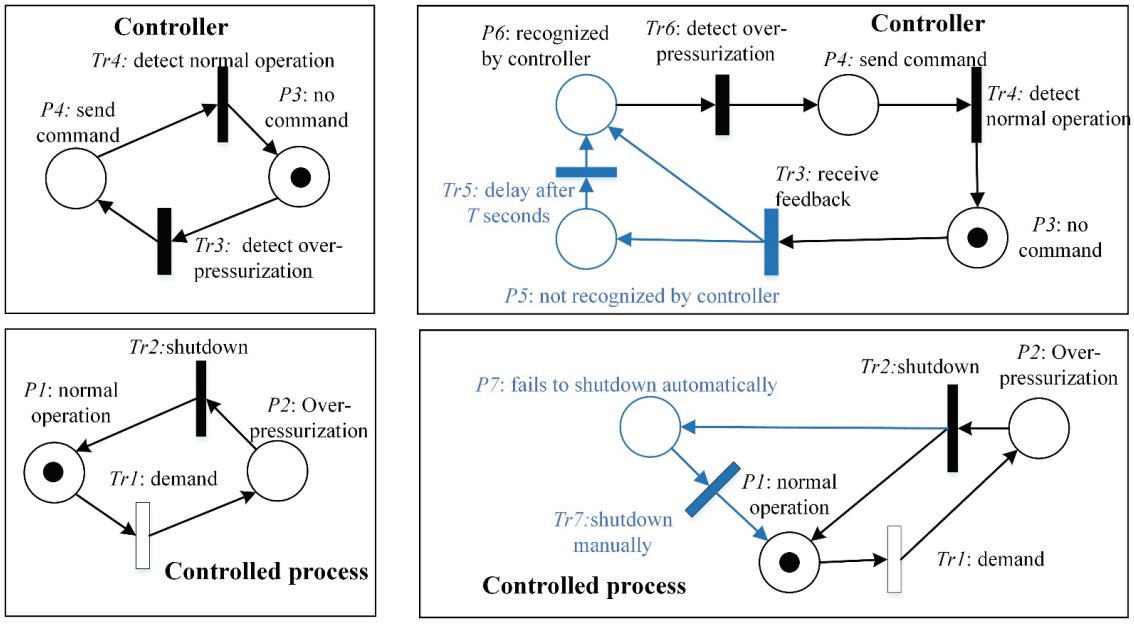
The proposed approach covers multiple models and the coordination between models are rather complex. The complexity here depends on the number of feedback control loops. The original feedback control loop defined in STPA is inadequate to express such complex coordination and has no execution ability. SPN that follow the state-event transition formalism is selected to structure models of proposed approach, without distorting the feedback control phenomenon of STPA. It may be noted that SPN is only one of many ways to visualize such interactions and construct the executable model. The other methods obeying state-transition formalism can achieve the same objective but they are not further discussed in this article.

3.2 Use SPN to construct STPA-RAM model

The SPN model consists of a *net structure* and a *marking* [35]. The net structure is made of the *places* (represented by circles), *transitions* (represented by bars), and their connection (presented by directed arcs). The arc links a place to a transition is called input arc and the arc links a transition to a place is called output arc, and they can be assigned with a natural number, named *weight* or *multiplicity* (normally assumed to be 1). Places may contain *tokens* (represented by bullet), which can move between places when enabled transition is fired. The transition is enabled when a number of token on each of its upstream places (a place connected by input arc) is not less than the weight/multiplicity of input arc. The transition is fired when the associated delay elapses (given that transition remain enabled during delays). The time delay between enabled transition and firing can be characterized as fixed or random [26]. The marking represents the distribution of tokens on a net structure. In such setting, the place of SPN can specify the context as premise condition for control action, and the tokens specify the state/value of context that decides whether the control action is needed or not. The transitions represent the control actions and information feedback on feedback control loop, and the time-dimension of control process is introduced by the random or fixed delays. In addition, *predicates* and *assertions* by means of variables can be introduced to SPN [36]. Predicate (often represented by '?') is a formula to validate/disable the transitions when variables are verified/unverified, and assertion (often represented by '!') is a formula to update the variables after the associated transition is fired. The predicates can model synchronization between control actions and controlled process, and the assertion is used to capture the transformational change in the system as the result of executed control actions. The detailed information about how to construct SPN model can be found in [28, 36]. The rest of this section introduces a small example for using SPN to construct STPA-RAM model.

Figure 4 illustrates a generic feedback control loop represented by SPN model. Two piecewise SPN models are structured to represent the behavior of controller and controlled process. The controlled process (i.e. system) can become abnormal and this is assumed as a stochastic process. The responsibility of controller is to intervene with the controlled process when it is in abnormal state, and system state is either maintained or, when relevant, reset to normal within the permitted time (X seconds). The two variables considered for predicates and assertions here are denoted as *normal_state* and *reset*.

Figure 4 (a) illustrates SPN model for the defined feedback control loop, assuming there is no loss scenario as the result of adequate control. The tokens initially stay in *P1* and *P3*, representing the state that the system is normal so no need to intervene the system. The initial marking is that one token stays in *P1* and one token stays in *P3*, indicating that normal state of system and no control command. When the token reaches *P2* from *P1* after firing the transition *Tr1* (i.e. system state becomes abnormal), the assertion of *Tr1* is '! *normal_state* =false'. Then, the transition *Tr3* is fired as the predicate of *Tr3* is '? *normal_state* =false', means that the controller sends the command to activate the system when abnormal state is detected (by controller). Similarly, when the token reaches *P4* through transition *Tr3*, the variable *reset* is assigned as *true* to fire the transition *Tr2* (i.e. send command to reset the system/controlled process). When the token leaves from *P2* to *P1* (means the activate process is completed after certain delay), the variable *normal_state* is updated as true so that transition *Tr4* can be fired.



(a) (b)

Figure 4 Mapping control structure into SPN: (a) adequate control and (b) two potential loss scenarios

Figure 4 (b) illustrates how we suggest modeling the influence of STPA output in SPN where two loss scenarios have been selected, and they are represented by net structure colored as blue. Loss scenario 1 is that controller sends the command too late (after *T* seconds) when abnormal state is detected, which leads to the hazard denoted as H.1. In this case, the transition *Tr3* in Figure 4 (a) is divided to two transitions *Tr3* and *Tr6* in Figure 4 (b) to distinguish between the event '*receive feedback of state*' and the event '*abnormal system state has been recognized (by controller)*'. In addition, two new places *P5* and *P6* are introduced to represent the context that '*feedback has been recognized too late*' and '*feedback has been recognized immediately*' respectively. The loss for H.1 is expressed as the extra *T* seconds that system is exposed to the abnormal state, equals to the delay of transition *Tr5*. Loss scenario 2 is that system is not successfully activated in response to the command and that a manual reset (intended to compensate) leads to hazard denoted as H.2. In this case, the transition *Tr2* in Figure 4 (a) is divided to two transitions *Tr2* and *Tr7* in Figure 4 (b) to distinguish between the event '*reset system upon control command*' and the event '*reset system manually*'. The new place *P7* is introduced to represent the state that '*the system fails reset automatically*'. The associated loss for H.2 is that the system is exposed to more stress when it is manually activated then the system is more prone to be abnormal in the rest of operation, saying that the transition rate of *Tr1* is slightly increased by α% after the transition of *Tr7*. The transition *Tr2* now has two downstream places: *P7* and *P1*. The frequency of loss scenario 2 can be denoted as the probability that token from *P2* enters into *P7* when transition *Tr2* is validated, that is '? *reset* =true'. Similarly, the frequency of loss scenario 1 can be denoted as the probability that token from *P3* enters into *P5* when transition *Tr3* is validated, that is '? *normal_state* =false'. Table 1 summarizes the synchronized product for Figure 4 (b).

Table 1 Synchronized product of case in Figure 4 (b)

Transition	Predicate	Assentation	Delay of transition
Tr1		normal_state=false	Stochastic delay, λ
Tr2	reset =true	normal_state =true	*X* seconds
Tr3	normal_state =false		0
Tr4	normal_state =true	reset =false	0
Tr5			*T* seconds
Tr6		reset =true	0
Tr7		$\lambda = \lambda \times (1+ \alpha)$	0

Although a quite simple and restrictive feedback control loop is considered in Figure 4, the above example is sufficient to illustrate how to construct STPA-RAM model by SPN. One specific issue is the refinement of SPN. The SPN in Figure 4 could be further refined by including SPN that represent sensor and actuator in the same feedback control loop or other actors from different feedback control loops. The coordination between actors are realized by the variables that are updated by assertion and propagated in feedback control loop by predicates. For instance, if the controller wrongly believes that the system is in abnormal state, a possible cause can be that the sensor provides the wrong feedback of actual state of system. To model this casual factor, one may construct another piecewise SPN that represent the evolution of sensor performance, e.g. *state_sensor*. The predicate of transition *Tr3* is subjected to the variable *normal_state* and *state_sensor*. The detailed example is given in the case study that follows in the next chapter.

4. CASE STUDY

In this section, the proposed approach is applied on a novel design concept of subsea architecture named Subsea Gate Box (SGB) that arises in Subsea Production and Processing SUBPRO [37] research center. The detailed introduction to this design concept can be found in [38]. Some simplifications are made on the original design concept for illustrative purpose. The modelling and simulation of SPN is completed by the software GRaphical Interface for reliability Forecasting (GRIF) [39] with the simulation engine Moca-RP.

4.1 System description

SGB is new field architecture concept where it is possible to install dedicated solutions for each well or a group of well considering the particular needs of subsea processing, i.e. boosting, metering and separation. The advantages of this design concept are in form of increasing oil and gas recovery, operation flexibility of separation and process efficiency. Figure 5 presents one alternative configuration for SGB, where each SGB consists of three functional modules: separation module (SPM), choke valve module (CVM) and multiphase pump (MPM) module. The normal processing line consists of SPM and MPM, where hydrocarbon flow is separated by SPM into liquid and gas, where the liquid is pumped through multiphase pump and the gas is assumed to flow naturally to the manifold. When the functional modules of the normal processing are faulty, the hydrocarbon can be bypassed to CVM on the same SGB. The choke valve then controls hydrocarbon pressure with low production efficiency. A subsea control system that interacts with the SGB equipment and sensors is vital for maintaining an optimal operation. The switch between processing lines is controlled by subsea controller (s) and realized by the open/close of crossover valve (XOV). SPM, MPM and CVM are retrievable. The connection between module (e.g. isolation valves and pipe connectors) and the sensors (e.g. transmitters of flow, temperature and pressure) are not illustrated in Figure 5.

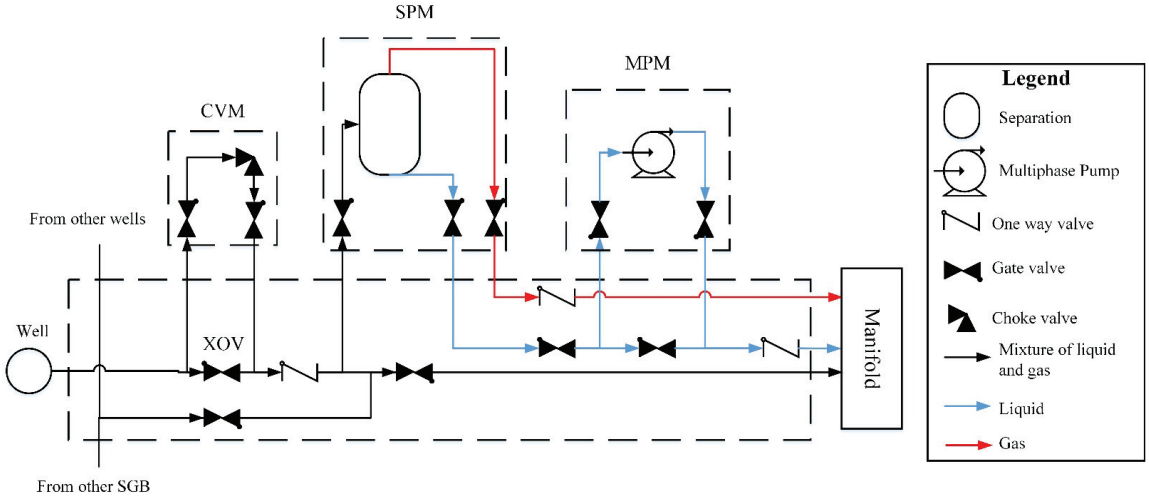


Figure 5 System schematic drawing of SGB

In the following subsections, the STPA-RAM model is constructed for illustrative purpose. The first step is to carry out STPA for analyzing the operating procedure of SGB. The involved actors for the control action are simplified as normal processing line (SGB-NP), bypass processing line (SGB-BP), XOV, sensor and controller. The second step is to build up RAM model considering the state of actors. Some data inputs for RAM models are assumed for demonstrating the approach only. Given the numerical results obtained through the STPA-RAM model, the countermeasures for selected loss scenarios are suggested. The selection of countermeasures are not discussed as the cost information for suggested measures are not available currently.

4.2 Step I: Carry out a general STPA

Based on the discussion with the system designer, three types of losses were identified: unexpected decrease in production efficiency (L.1), hydrocarbon spills (L.2), and complete shutdown of SGB (L.3). The associated system level hazards and associated constraints are summarized in Table 2.

Table 2 System-level hazards and constraints for SGB

System level hazard (SH)	**System-level constraints (SC)**
SH.1: Hydrocarbons flow into non-optimal processing line [L.1]	SC.1 Hydrocarbons must always flow into optimal processing line
SH.2: Hydrocarbons flow into unavailable processing line [L.1, L.2, L.3]	SC.2 Hydrocarbons must never flow into unavailable processing line
SH.3: Over-pressurization of equipment in selected processing line [L.2, L.3]	SC.3 Pressure must never be built-up above design limit

The high-level hierarchical control structure is illustrated in Figure 6. The subsea controller consists of process control system (PCS), subsea control unit (SCU), process shutdown system (PSD), subsea control module (SCM) and subsea electronic module (SEM). The structure and complexity of subsea controller depend on the operating strategies and distance to controlled equipment [15]. For instance, PCS and PSD located on surface facility deliver the command from human operator to control equipment and shut down the system, through SCU to the SCM/SEM that located subsea. To simplify the case study, only SCM and SEM are considered, and the responsibility is distribute the control commands to equipment. When the ability to use

the normal processing line is lost, human operator sends the coded command to SCM/SEM that distributes the command to associated valves. The SGB-NP is shut down by the closure of isolation valve, and XOV is opened thus the hydrocarbon is redirected to CVM with lower production efficiency. When the normal processing line is restored after maintenance, then human operator sends the command through the similar process to restart SPM and MPM and redirect flow to normal processing line.

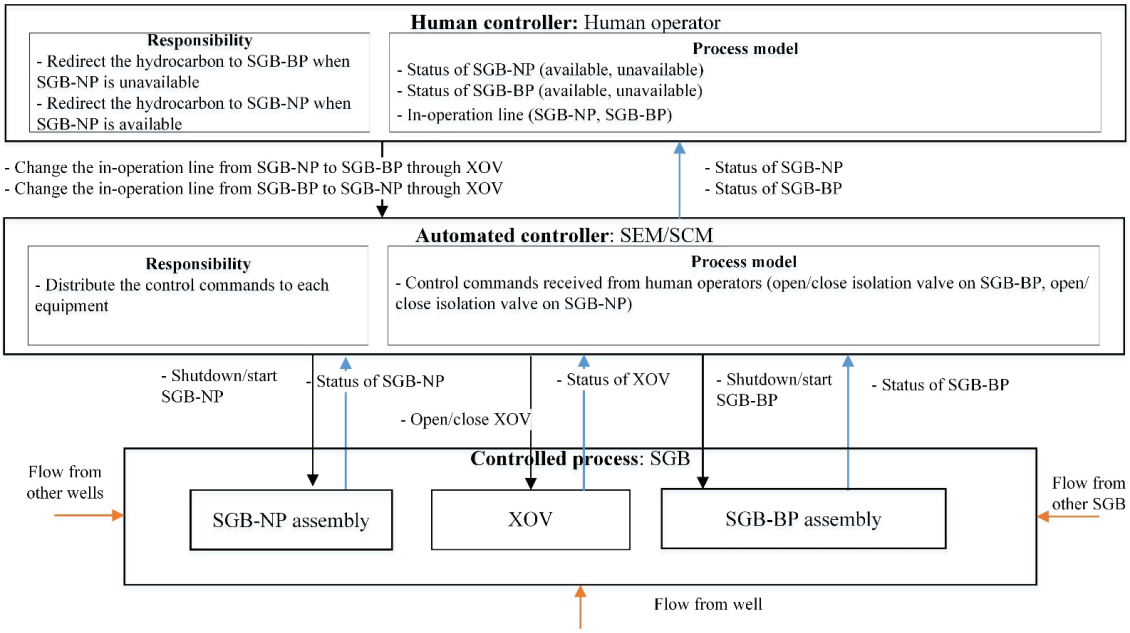


Figure 6 High-level control structure of SGB

On the basis of control structure defined above, we identified UCAs. Some examples are reported in Table 3. The loss scenarios (SO) can be further identified (here using UCA.1 as example) as reported in Table 4. In addition, Table 5 identifies the loss scenarios related to the situation that human operator sends the correct control command to change from SGB-NP to SGB-BP but it is not followed or improperly followed by automated controller. It is assumed that some suggested countermeasures in Table 4 and Table 5 have been derived from analyses carried out for the purpose of this article. It is expected that more detailed analysis with improved results would come with an updated analysis when the SGB has reached a more mature design stage.

Table 3 UCAs for defined control structure

<table>
<tr><th>Control action from SEM/SCM</th><th colspan="4">Identification of UCAs</th></tr>
<tr><td rowspan="2">Change the in-operation line from SGB-NP to SGB-BP through XOV</td><td>Not provided</td><td>Provided</td><td>Wrong timing or order</td><td>Too soon or too long</td></tr>
<tr><td>UCA.1: Control command is not provided when SGB-NP is faulty and XOV is available [SH.1, SH.2,]</td><td>UCA.2: Control command is provided when both SGB-NP and XOV are available [SH.1]
UCA.3: Control command is provided when both SGB-NP and SGB-BP are faulty [SH.1, SH.2]</td><td>UCA.4: Control command is provided too late when SGB-NP is faulty and XOV is available [SH.2, SH.3]</td><td>UCA.5: Control command is stopped too soon before XOV is fully closed when SGB-NP is faulty [SH.2, SH.3]</td></tr>
</table>

Table 4 Loss scenarios related to UCA.1 and suggested countermeasures

UCA.1: Change the in-operation line from SGB-NP to SGB-BP through XOV is not provided by SCM/SEM on command from human operator when SGB-NP is faulty and XOV is available [SH.1, SH.2]	
Loss scenarios	**Suggested countermeasures**
SO.1 for UCA.1: Human operator receives correct feedback but interprets it incorrectly so SEM/SCM does not receive control command from human operator. The causal factor is that human operator lacks sufficient understanding for abnormal situation.	Must provide the sufficient training for operators to deal with specified hazardous situations.
SO.2 for UCA.1: Human operator receives correct feedback but makes mistakes so SEM/SCM does not receive control command from human operator. The causal factor is that human operator is overstressed when there are too many process to be considered.	The reference document must be presented to provide guidance for operation.
SO.3 for UCA.1: Human operator receives incorrect feedback about conditions of SGB-NP so wrongly believes that the SGB-NP is working but it is not. The casual factor is that the sensor on SGB-NP provides erratic readings.	Sensors must be monitored continuously and be calibrated when erratic reading was detected

Table 5 Detailed loss scenarios and suggested countermeasures

Loss scenarios	**Suggested countermeasures**
SO.4: The control command is initiated by human operator but not received by SCM/SEM. The casual factor is that there is a critical failure on SEM/SCM [SH.1, SH.2].	The status of SCM/SEM must be checked before operation and after each updates.
SO.5: The control command is provided by SCM/SEM on command from human operator, but actuator does not responds to this control command. The casual factor is critical failures on XOV (actuator) [SH.1, SH.2].	XOV must be checked regularly and be repaired when critical failure is revealed.

The suggested countermeasures may degrade or become less efficient considering operating conditions of SGB. For instance, the availability of XOV cannot be guaranteed by continuously monitoring and repair due to maintenance in subsea context may be delayed considering the availability of vessel that transport spare parts. In addition, the cost of some suggested countermeasures may be considerable. For instance, monitoring potential faults in sensor measurements often requires a reference sensor to be installed with additional costs for purchasing and installation. Therefore, designers would like to evaluate the cost-benefit before selecting countermeasures. In this case study, two loss scenarios that caused by erratic reading on sensors are investigated to exemplify:

- Loss scenario 1 (LSO1): Human operator receives incorrect feedback about conditions of SGB-NP due to erratic readings of sensor and wrongly believes that the SGB-NP is faulty but it is not. The control command to stop SGB-NP and activate SGB-BP is provided accidently (SH.1). It is assumed that this situation is recognized after 360 hours and the system operates in reduced production efficiency during this period (L.1).

- Loss scenario 2 (LSO2): Human operator receives incorrect feedback about conditions of SGB-NP due to erratic readings of sensor and wrongly believes that the SGB-NP is working but it is not. The control command to stop SGB-NP and activate SGB-BP is not provided so SGB-NP is not stopped timely (SH.1, SH.2). It is assumed that this situation is recognized almost immediately, but the system must be shut down (L.1, L.2 and L.3) until it can be restored through maintenance.

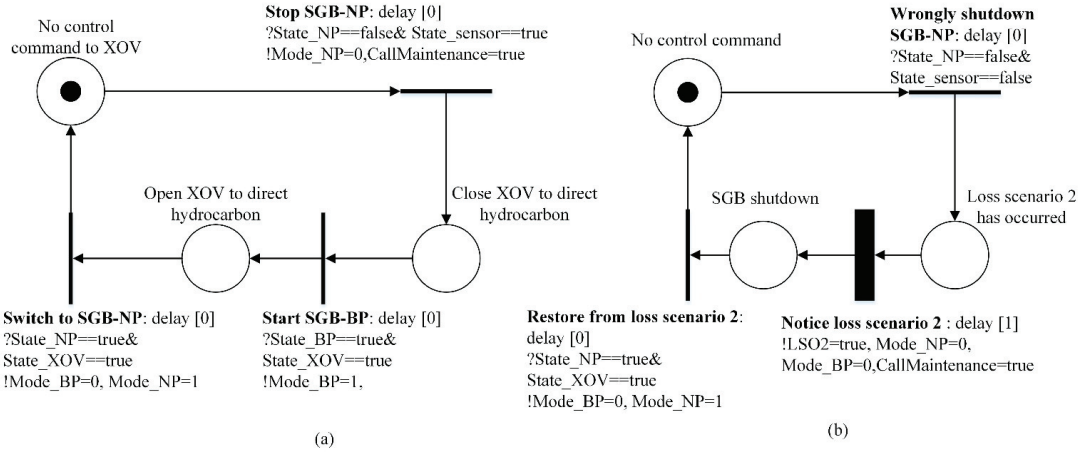


Figure 7 Mapping safe scenario and loss scenario 2 into SPN models

Figure 7 illustrates SPN for the safe scenario in (a) and loss scenario 2 in (b). The safe scenario is that the control command is provided correctly to switch from SGB-NP to SGB-BP in presence of failure of SGB-NP. Once the failure has been detected, the preparation of maintenance can start (!*CallMaintenance*=true) and SGB-NP is stopped (!*Mode_NP*=0). If both SGB-BP and XOV are available, then the processing line is switched to SGB-BP (!*Mode_BP*=1). After maintenance is completed, hydrocarbon is redirected to normal processing line as the faulty SGB-NP, SGB-BP and XOV is replaced. The loss scenario 2 can occur when sensor provide incorrect feedback (?*State_sensor*==false) in together with failure on SGB-NP (?*State_NP*==false). This loss scenario is immediately detected after 1 hour and the system is shutdown (!*Mode_BP*=0, *Mode_NP*=0, *SO2*=true) and preparation of maintenance start (!*CallMaintenance*=true). After maintenance is completed, the system is restored in the same way as safe scenario. SPN model for loss scenario 1 can be also generated in the similar way. It is assumed that variables related to loss scenarios and safe scenario (State_sensor, State_XOV, State_NP, State_BP) are subjected to system evolution and interventions, which is described by the RAM model. The variables *Mode_BP* and *Mode_NP* indicate whether there are hydrocarbon flows into the available processing line or not. These two variables are defined in integral domain, whereas the other variables are defined in Boolean domain.

4.3 Step II: Develop RAM models for selected loss scenarios

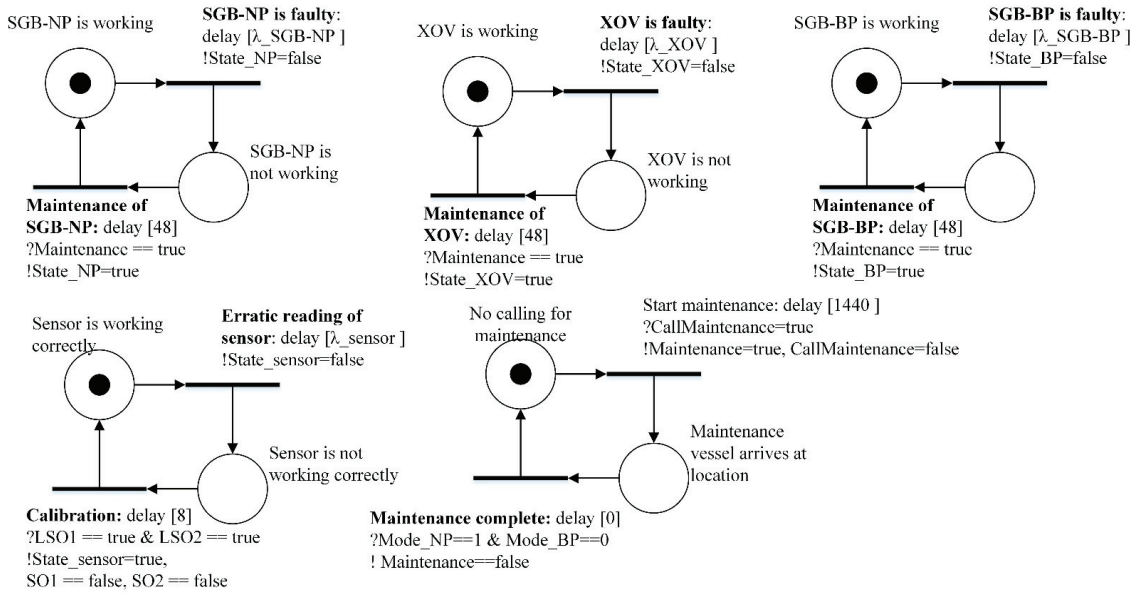


Figure 8 SPN model for maintenance and evolution of controlled process

Figure 8 presents SPN model for related variables. The maintenance of hardware component (i.e. SGB-NP, SGB-BP and XOV) is completed together after a certain delay (1440 hours), so the variable *Maintenance* is introduced to synchronize the maintenance events on different piecewise SPN. Since it is assumed that there is no means to reveal the erratic readings on sensor, the sensor is updated through on-line program after 8 hours once both loss scenarios have been recognized (?*LSO1*==true & *LSO2* ==true).

The reliability data for subsea equipment retrieved from the database OREDA [40] are re-evaluated based on discussion with system designer considering the novelty of technology and operating conditions. The estimated data, assumptions and computational setting are as follows:

1) The status of SGB-NP, SGB-BP and XOV is assumed to be under continuously monitoring, thus the failure is immediately revealed. The failure rates for SGB-NP, SGB-BP and XOV are assumed as 3×10^{-5} hour^{-1}, 1×10^{-5} hour^{-1} and 1.5×10^{-6} hour^{-1} respectively. All the failure events are assumed to be exponentially distributed. The sensor is assumed to continuously provide the feedback that is possibly erratic. To compare various control strategies, the four sets of transition rates for this failure mode are assumed as:
    - Case 0: occurrence rate for erratic reading =0
    - Case 1: occurrence rate for erratic reading =0.5×10^{-5} hour^{-1}
    - Case 2: occurrence rate for erratic reading =1×10^{-5} hour^{-1}
    - Case 3: occurrence rate for erratic reading =1.5×10^{-5} hour^{-1}
2) System run with 55% production efficiency when SGB-BP is active.
3) The time for mobilization is 1440 hours. The time of retrieval and reinstallation is delayed for 48 hours. The faulty equipment is replaced (as good as new after maintenance) and the working equipment keeps running as it is (as bad as old after maintenance).

4) The experiment time for simulation is 10 years (i.e. 87600 hours). 5×10^5 simulation runs have been used for each case. The computation time was approximately 44 minutes with a 2.60 GHz processor, 16 GB of RAM, and it can increase if there are more variables to observe.

4.4 Numerical results

The frequency of loss scenarios was calculated by observing the frequency of related transitions in SPN, as reported in Table 6. Loss scenario 1 only lead to SH.1, which in worst condition can lead to the production loss (L.1). Loss scenario 2 can lead to all three system-level hazards, which in worst condition can lead to production loss (L.1, L.3) and the hydrocarbon spills accident (L.2). The costs for associated consequence of L.2 given the emergency barrier management can be estimated through event tree analysis.

Table 6 Frequency of loss scenario 1 and 2

	Loss scenario 1 (L.1)	**Loss scenario 2 (L.1, L.2, L.3)**
Case 1	7.028×10^{-2} year^{-1}	3.3×10^{-4} year^{-1}
Case 2	1.427×10^{-1} year^{-1}	5.7×10^{-4} year^{-1}
Case 3	2.033×10^{-1} year^{-1}	7.9×10^{-4} year^{-1}

The effect of loss scenarios on production loss can be directly calculated through simulation. Figure 9 and Figure 10 illustrate the average value of system production deficiency and system unavailability from 0 to t, respectively.

The system production deficiency is stated as below:

$$100\% - (Mode\_BP \times 55\% + Mode\_NP)$$

And system unavailability equals to:

$$1 - (Mode\_BP + Mode\_NP)$$

Where the initial value for variable *Mode_NP* is 1, whereas *Mode_BP* is assumed to be 0 as bypass processing line is not working in the beginning of operation.

Case 0 shows the situation that the adequate control has been provided for loss scenario 1 and 2, therefore only the safe scenario has been considered. As reported in Table 6, the frequency of loss scenario 1 seems as proportional to the occurrence rate for erratic reading, whilst loss scenario 2 is not. The reason is that loss scenario 1 is subjected to unavailability of sensor (that is proportional to the occurrence rate for erratic reading) and availability of SGB_NP, whereas loss scenario 2 is subjected to unavailability of sensor and unavailability of SGB_NP. The availability of SGB_NP can be seen as proportional to the occurrence rate for erratic reading due to the impact of maintenance in both safe scenario and loss scenario 2, whilst unavailability of SGB_NP is not.

The average unavailability and production deficiency in case 0 are 0.0057 and 2.14%, whereas in worst case (case 3) are 0.0148 and 3.08%. If assume that SGB can produce 2 million kroner worth oil and gas per day or 730 million Norwegian kroner (NOK) per year, then the expected difference between case 0 and case 3 is 6.862 million NOK per year in stakeholder's favor.

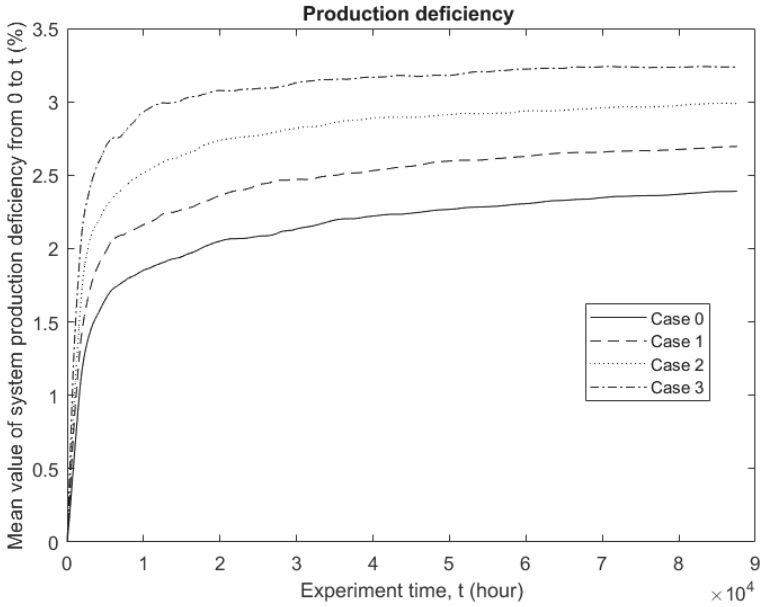


Figure 9 System production deficiency of case 0-3

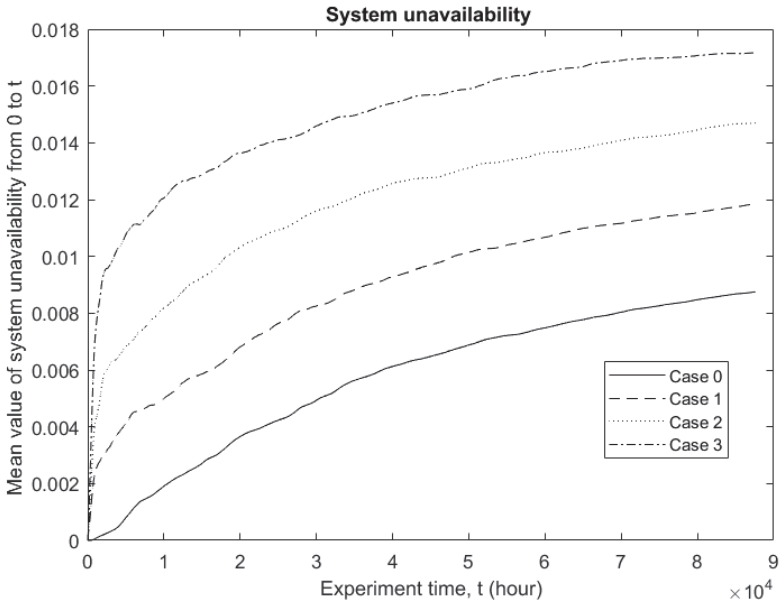


Figure 10 System unavailability of case 0-3

It is observed that the effect of loss scenarios is considerable, according to their impact on production and potential for severe accident like hydrocarbon spills. Some example countermeasures are suggested as following:

- Preventive countermeasure is to reduce the transition rate to the state that sensor has the erratic reading. For example, the validity and accuracy of signals from sensors can be increased by removing noise from piping conditions.
- Compensating countermeasure is to increase the ability of controller to discriminate between a real demand and false demand caused by erratic readings provided by sensor. For instance, installation of master sensor that monitors and compares the reading of duty sensor.
- One may also notice that the loss scenario 1 has much less severe consequence but high frequency than loss scenario 2. The system designer may consider to start troubleshooting once loss scenario 1 has been recognized. The premise condition for loss scenario 2 can be removed in this situation since they share the same casual factor and these two loss scenarios cannot occur simultaneously. This said, the hidden error in sensor is revealed and subsequently corrected by a demand.

The selection of compensating and preventive countermeasure depends on frequency of loss scenarios obtained through STPA-RAM modelling and the cost estimation for adverse effects and perceived benefits, where the later one is beyond the scope of this article.

5. DISCUSSION

This article proposes a new approach to combine STPA and RAM models, with support of existing modelling formalism SPN. The new approach is made of fundamental elements of each method, to take advantage of each strength whilst to compensate for their weakness. In this respect, the contributions are twofold: (1) to address uncertainty in STPA so its results can be confidently used by decision makers (2) to improve the construction of SPN model taking advantage of control structure offered by STPA.

5.1 Level of uncertainty

The proposed approach enables the quantification of hazards derived by a relatively new method STPA, and thereby improve the possibility for decision-making about design choices. It is reasonable to ask to what extent we have succeed in this respect. The level of uncertainty is of relevance for making such judgement. In this respect, uncertainty for STPA-RAM model can be categorized into *completeness uncertainty* that stems from stems from incomplete scope of hazard identification, *model uncertainty* that stems from low suitability of modelling formalism and *data uncertainty* that stems from improper selection of distribution and associated parameter values [41], as illustrated in Figure 11.

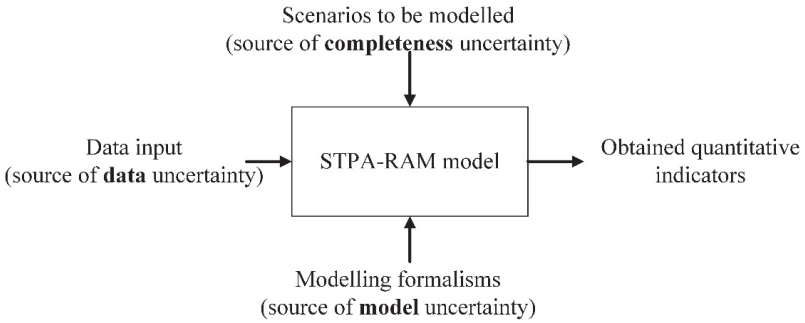


Figure 11 Uncertainty related to STPA-RAM model

As discussed earlier, human errors and software errors become visible in STPA when they are properly defined in the feedback control loop. This feature ensures STPA to develop a (theoretically) complete spectrum of scenarios, where the term complete of course depends on the purpose of analysis as done in step 1 of STPA. When the detailed study of STPA is conducted, it is often to get hundreds of UCAs and thousands of loss

scenarios. It is practically impossible to include them in one single STPA-RAM model due to a significant increase in computational burden. The pre-processing methods for STPA-RAM model in this sense are required, for example to eliminate loss scenarios based on existing and planned safety barriers as suggested in [14], or to prioritize loss scenarios based on criticality or risk measures. If the rationales behind these pre-processing methods are specified and documented, the category of completeness uncertainty is reduced.

SPN with predicates and assertions can model loss scenarios without distorting the phenomenon of control structure. The reason is that the use of predicates and assertions using variables can introduce the guard for transitions, which is equivalently the context for safe or unsafe control actions. If the user of STPA-RAM model is competent and aware of the limitation of employing SPN, the model uncertainty of STPA-RAM model is well acknowledged.

The major bottleneck for STPA-RAM model seems to be data uncertainty. The reason is that the loss scenarios derived by STPA move beyond the failure scenarios as the combination of failure modes, whereas most of data resource collect and record data on basis of failure modes. The probabilistic modelling of loss scenarios is therefore greatly relied on the expert judgement and engineering experience. Rather than abandoning probabilistic model, Berner and Flage [42] elaborated a solution to evaluate the strength of background knowledge and beliefs about assumption deviations as supplement to the use of probability tools. The confidence or data uncertainty of STPA-RAM model therefore depends on the description of background knowledge that judges and justifies the judgement about assumptions and simplification made. This is remarked as the future work as the potential improvement to the proposed approach.

5.2 Pattern-wise model construction

When dealing with a complex system, it often occurs that a large scale SPN model is constructed and remains unreadable and unmanageable [36]. The reason may be the lack of proper description model before constructing SPN model so the construction mainly relies on the imagination of model designer. STPA in this sense can facilitate the model construction of SPN model. The behavior (e.g. failure) of components can be classically modelled by piecewise SPN model.

The remaining question is about how to model the complex maintenance process as control loops, especially for predictive maintenance with the enhanced level of digitalization. Here we propose to model such complex maintenance process as a feedback control loop advocated in STPA: the decision on maintenance is considered as a controller of some sort, the feedback for making decisions are for example the degradation level of component, the control action is therefore to change the state of components for example notifying personnel of maintenance/replacement of equipment. The complex maintenance process is then modelled as a pattern in SPN, for example as shown in Figure 8. The interfaces of maintenance process to other patterns are representing by global variables (e.g. Mode_BP and Mode_NP in Figure 8).

With such process, we can produce the patterns of different control loops and they can be replicated as many times as need, and make the large-scale SPN model more compact and understandable. By translating description model into SPN model, the causality knowledge can be traceable and updated when hierarchical control structure is updated (for example from step 2 to step 4 in an original STPA procedure). More importantly, when there is more than one hierarchical control structure, we can use the same process to synthesize them and complete in a one single model if necessary. In this regard, we argue that STPA can facilitate constructing SPN model, and this feature makes STPA-RAM model more appealing for systems with complex maintenance processes.

5.3 Limitation and constraints

One limitation of the case study is that the loss scenarios selected for the numerical experiment in this paper would normally be identified by traditional failure mode analysis methods. Several authors claim that STPA is able to identify more hazards than traditional failure modes identification method, with regard to software error and interaction type of hazards [8, 10, 18]. For example, one complex loss scenario for SGB design case

could be: ‘human operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass processing line, due to a long procedure taken before giving decision or SCU delays in the processing of command to adjust set point of choke valve’. This loss scenario can be prevented by either updating operating procedures (e.g. the procedure must be done within appropriate amount of time) or modifying the design (e.g. SCU must be able to process the control command immediately).

Another limitation of the case study is the intentional exclusion of software flaws and human errors. One reason behind is that human errors and software flaws are often judged as systematic factors that must be removed before operation as required in standards, e.g. functional safety standard IEC 61508 [43]. Another reason is the lack of relevant database, implies a great dependence on expert judgements and operational experience. If relevant data is available and the related loss scenarios are judged as critical (e.g. poor knowledge and operating experience), STPA-RAM model can include the effect of human and software error to evaluate how they contribute to the frequency of loss scenarios. The interesting part is that learning pattern for software and human [22]. It means that human or software can learn from experience, and same hazards are avoided under the associated context. Taking the Figure 4 (b) as example, the casual factors considered for loss scenario ‘sending control command too late’ could be the inadequate understanding of unscheduled situations occur. One can assume that the process model of controller can be improved through the lesson learnt. Therefore, the assertion of Tr5 is ‘!T=T×0.5’ to coarsely model this situation that the delay of detecting abnormal signal is decreased every time this loss scenario happens.

In case study, only two loss scenarios are modelled. Even some methods for elimination and prioritization of loss scenarios, the number of critical loss scenarios is likely to be more than that. Each loss scenario, or a combination of a few, is regarded as testing experiments of different operational situations. Despite our approach taken, it is interesting to investigate strategies for including more loss scenarios in the same model, when this is needed.

In some applications, the evolution of controlled process may be subjected to the shocks from environment, which is not modelled statistically. For instance, if the case study is further refined to study the performance on SPM, then the process variables like liquid level on separator is considered. This process variable is determined by the control command (e.g. open/close liquid discharge valve) and the environmental disturbance (e.g. flow conditions from wells). The change of state of latter one is less predictable than the first one that is subjected to stochastic event. The potential solution for this problem may be to integrate STPA-RAM model with the model that studies the physics of controlled process, e.g. finite element analysis. The simulation time is therefore greatly amplified by the agility of process variables, which make the proposed approach unappealing when comes to the industry-scale system.

6. CONCLUSION

This article has discussed the potential interface between STPA as qualitative analysis and RAM models as means for quantification. It is argued that qualitative analysis is still needed to interpret the loss scenarios derived from STPA. In this respect, an integrated approach that combines the STPA and RAM model through SPN that follow state-event transition formalism is proposed. In the case study, it has been shown that the STPA-RAM model can quantitatively calculate the frequency of loss scenarios by combing with prepared RAM models. The numerical results give risk-based insights to system production, maintenance and emergency management, and some countermeasures are suggested accordingly. We conclude that the proposed approach is a way to connect between STPA and RAM models. This approach helps to clarify to what extent STPA can contribute to decision-making in an engineering design, e.g. the design of safety barrier and IMR strategies.

Future work includes to evaluate the background knowledge and sensitivities of assumptions made for probabilistic models, so the confidence of STPA-RAM model can be judged by decision makers. Some approaches have been discussed in [42]. The next step is then to fuse it into the approach proposed in this article. In addition, current framework of proposed approach focuses primarily on the side of constructing

model for simulation, but few attention has been paid to balance the simplicity and expressiveness of STPA-RAM model. Another important area of further research is therefore to develop approach to screen out and prioritize the loss scenarios. One possible strategy is to evaluate the effectiveness of safety constraints in terms of its availability and easiness of implementation, as well as the criticality of associated losses. This may require not only the advance in analytical methods, but also the multidisciplinary participations for conducting STPA to seek multiple perspectives for prioritization.

AKNOWLEDGEMENT

This work was carried out as a part of SUBPRO, a research-based innovation center within Subsea Production and Processing. The authors gratefully acknowledge the project support, which is financed by the Research Council of Norway, major industry partners and NTNU. Our special thanks to the industry partner DNV-GL inside SUBPRO, who contributes to this body of knowledge and provides inspirations on current issues facing in the post-processing of STPA.

REFERENCE

[1]. Bai, Y. and Q. Bai, *Subsea Engineering Handbook*. 2010, Boston: Gulf Professional Publishing. xxv.
[2]. Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety*. 2011: MIT Press.
[3]. Abdulkhaleq, A., S. Wagner and N. Leveson, *A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA.* Procedia Engineering, 2015. **128**: p. 2-11.
[4]. Rasmussen, J., *Risk management in a dynamic society: a modelling problem.* Safety Science, 1997. **27**(2): p. 183-213.
[5]. Seligmann, B.J., E. Németh, K.M. Hangos and I.T. Cameron, *A blended hazard identification methodology to support process diagnosis.* Journal of Loss Prevention in the Process Industries, 2012. **25**(4): p. 746-759.
[6]. Hollnagel, E., *FRAM:The functional resonance analysis method:modelling complex socio-technical systems*. 2012 Farnham: Ashgate Publishing Ltd.
[7]. Leveson, N. and J. Thomas, *STPA handbook* 2018: MIT.
[8]. Mahajan, H.S., T. Bradley and S. Pasricha, *Application of systems theoretic process analysis to a lane keeping assist system.* Reliability Engineering & System Safety, 2017. **167**: p. 177-183.
[9]. Kim, H., M.A. Lundteigen, A. Hafver, F. Pedersen and G. Skofteland, *Application of Systems-Theoretic Process Analysis to isolation of subsea wells: opportunities and challenges of applying STPA to subsea operation*, in *Offshore Technology Conference*. 2018: Houston, Texas, USA.
[10]. Sulaman, S.M., A. Beer, M. Felderer and M. Höst, *Comparison of the FMEA and STPA safety analysis methods–a case study.* Software Quality Journal, 2017.
[11]. Abdulkhaleq, A., D. Lammering, S. Wagner, J. Röder, N. Balbierer, L. Ramsauer, T. Raste and H. Boehmert, *A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles.* Procedia Engineering, 2017. **179**(Supplement C): p. 41-51.
[12]. Faiella, G., A. Parand, B.D. Franklin, P. Chana, M. Cesarelli, N.A. Stanton and N. Sevdalis, *Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach.* Reliability Engineering & System Safety, 2018. **169**(Supplement C): p. 117-126.
[13]. Nakao, H., M. Katahira, Y. Miyamoto and N. Leveson. *safety guide design of crew return vehicle in concept design phase using STAMP/STPA*. in *Proceeding of the 5th IAASS Conference* 2011. Citeseer.
[14]. Rokseth, B., I.B. Utne and J.E. Vinnem, *A systems approach to risk analysis of maritime operations.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2016. **231**(1): p. 53-68.
[15]. Kim, H., M.A. Lundteigen, A. Hafver, F. Pedersen, G. Skofteland, C. Holden and S.J. Ohrem, *Application of Systems-Theoretic Process Analysis to a Subsea Gas Compression System*, in *ESREL* 2018: Trondheim, Norway.
[16]. Young, W. and N. Leveson, *Systems thinking for safety and security*, in *Proceedings of the 29th Annual Computer Security Applications Conference*. 2013, ACM: New Orleans, Louisiana, USA. p. 1-8.
[17]. Friedberg, I., K. McLaughlin, P. Smith, D. Laverty and S. Sezer, *STPA-SafeSec: Safety and security analysis for cyber-physical systems.* Journal of Information Security and Applications, 2017. **34**: p. 183-196.
[18]. Rodríguez, M. and I. Díaz, *A systematic and integral hazards analysis technique applied to the process industry.* Journal of Loss Prevention in the Process Industries, 2016. **43**: p. 721-729.
[19]. Wróbel, K., J. Montewka and P. Kujala, *System-theoretic approach to safety of remotely-controlled merchant vessel.* Ocean Engineering, 2018. **152**: p. 334-345.
[20]. Hafver, A., S. Eldevik, I. Jakopanec, O.V. Drugan, F. Pedersen, R. Flage and T. Aven, *Risk-based versus control-based safety philosophy in the context of complex systems*. 2017. 38-38.
[21]. Rausand, M. and A. Høyland, *System Reliability Theory, Models, Statistical Methods, and Applications*. second edition ed. Hoboken, NJ. 2004: John Wiley & Sons, Inc. 419-464.

[22]. ISO/TR 12489, *Petroleum, petrochemical and natural gas industries -- Reliability modelling and calculation of safety systems*. 2013, Geneva: International Electrotechnical Commission.
[23]. Innal, F., *Contribution to modelling safety instrumented systems and to assessing their performance: Critical analysis of IEC 61508 standard, PhD Thesis*. 2008, Bordeaux: University of Bordeaux
[24]. IEC61165, *Application of Markov techniques*. 2006.
[25]. IEC 62551, *Analysis techniques for dependability - Petri net techniques*. 2012.
[26]. Marsan, M.A., G. Balbo, G. Chiola, G. Conte, S. Donatelli and G. Franceschinis, *An introduction to generalized stochastic Petri nets.* Microelectronics Reliability, 1991. **31**(4): p. 699-725.
[27]. Rauzy, A., *Guarded transition systems: A new states/events formalism for reliability studies.* Proceedings of the Institution of Mechanical Engineers. Part O, Journal of risk and reliability, 2008. **222**(4).
[28]. Signoret., J.-P., *Dependability & Safety Modeling and calculation: Petri Nets*, in *In Proceeding of the 2nd IFAC Workshop on Dependable Control of Descrete Systems*. 2009: Bari, Italy.
[29]. Wang, R., W. Zheng, C. Liang and T. Tang, *An integrated hazard identification method based on the hierarchical Colored Petri Net.* Safety Science, 2016. **88**: p. 166-179.
[30]. Dirk, S., H. René Sebastian, W. Jan and S. Eckehard, *Integration of Petri Nets into STAMP / CAST on the example of Wenzhou 7.23 accident.* IFAC Proceedings Volumes, 2013. **46**(25): p. 65-70.
[31]. Rokseth, B., I.B. Utne and J.E. Vinnem, *Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis.* Reliability Engineering & System Safety, 2018. **169**(Supplement C): p. 18-31.
[32]. Leveson, N. and J. Thomas, *STPA primer version 1*. 2013.
[33]. Bjerga, T., T. Aven and E. Zio, *Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM.* Reliability Engineering & System Safety, 2016. **156**(Supplement C): p. 203-209.
[34]. Thomas, J., *Extending and Automating STPA for Requirements Generation and Analysis, Ph.D. Dissertation*. 2013: MIT.
[35]. Balbo, G., *Introduction to Generalized Stochastic Petri Nets*, in *Formal Methods for Performance Evaluation: SFM*, M. Bernardo and J. Hillston, Editors. 2007, Springer Berlin, Heidelberg. p. 83-131.
[36]. Signoret, J.-P., Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas and P. Thomas, *Make your Petri nets understandable: Reliability block diagrams driven Petri nets.* Reliability Engineering & System Safety, 2013. **113**: p. 61-75.
[37]. SUBPRO, *Subsea production and processing*. 2015: https://www.ntnu.edu/subpro.
[38]. Diaz, M.J.C., M. Stanko and S. Sangesland, *Exploring New Concepts in Subsea Field Architecture*, in *Offshore Technology Conference*. 2018.
[39]. GRIF, *Graphical Interface for reliability Forecasting*. 2016, France: SATODEV.
[40]. OREDA, *Offshore and Onshore Reliability Data, 6th edition*. 2015.
[41]. NUREG-1855, *Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making*. 2009: Nuclear Regulatory Commision
[42]. Berner, C. and R. Flage, *Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions.* Reliability Engineering & System Safety, 2016. **151**: p. 46-59.
[43]. IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety related systems. Part 1-7*. 2010, Geneva: International Electrotechnical Commission.