NTNU

Norwegian University of
Science and Technology

Prioritization Approach for Systems-Theoretic Process Analysis (PA-STPA) : Applied for Subsea Systems

Nanda Anugrah Zikrullah

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2018
Supervisor: Mary Ann Lundteigen, MTP
Co-supervisor: Hyungju Kim, MTP

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

Preface

This report is written by master student in RAMS, Nanda Anugrah Zikrullah. It represents master thesis work from RAMS at NTNU as part of the study program TPK4950 - RAMS Master's Thesis. It is performed in collaboration with SUBPRO research center as part of the development of the Subsea Gate Box. Two works related to this research has been performed during the summer and autumn semester of 2017.

The thesis is a continuation of previous internship research and specialization project performed by the same author for SUBPRO. This thesis title is "Prioritization approach for systems-theoretic process analysis (PA-STPA): applied for subsea systems".

The target of this report is directed to people who are using STPA for the hazard analysis tool. People may also be benefited by the increase in efficiency from the analysis. Readers unfamiliar with the subject may refer to the literature study provided and the reference given in each section.

Trondheim, 2012-12-10

Nanda Anugrah Zikrullah

Acknowledgment

I would like to thank Professor Mary Ann Lundteigen and Postdoc Hyungju Kim from NTNU and SUBPRO for their good advice and continuous supports during the development of this research. Without their guidance, this thesis would not have been possible.

I would like to thank Postdoc Mariana J.C. Diaz Arias for her insight on developing the system served as the study case for this research. Clear and detail explanation given during the presentation increased the easiness for development of system description used in the study case.

I would like to thank The SUBPRO research center for the opportunity to have an internship throughout the summer 2017. The internship provided the chance to meet up with different researcher from similar fields which become the reference for discussion to develop the project.

I would also like to thank Frank Børre Pedersen and Andreas Hafver from DNV-GL for their critical comments during the development of the approach. Their expertise gave me different views that could complement my research.

Additional thanks should be given to some friends from Indonesia and RAMS which help me for their support through the duration of the research, not only from the formal work, but also during the leisure activity which maintained my spirits to give the best for the thesis.

Final thanks had to be given to my father, Dwi Darmawanta Hartadjaja, and my mother, Ninik Joeniwati, for their spiritual support throughout the work.

N.A.Z.

Abstract

A considerable amount of scenarios and constraints were produced by the basic systems-theoretic process analysis (STPA) application. It increased the difficulty to allocate resources for problem-solving. While these problems also applied to all other traditional hazard analysis tools, only STPA had not implement prioritization in the process. The purpose of this study is to develop a prioritization approach for STPA.

Prioritization approach for systems-theoretic process analysis (PA-STPA) was proposed based on risk-based decision making (RBDM) approach. The proposed approach consisted of five main steps, four main steps from the basic STPA process and one additional step for solution proposal. Additionally, assessment processes were added to each step to quantify the qualitative assessment results. The obtained values were used to rank the results.

PA-STPA has been applied to "the subsea gate box (SGB)" system and compared to the result from basic STPA. The study found that PA-STPA had higher analysis efficiency than basic STPA process while having the risk of reducing the safety level of the results by screening out high risk scenarios. This effect might differ, depending on the unsafe control action (UCA) screening criteria used.

The subjectivity of the assessment, formula used for calculation and result safety issue had been identified as weaknesses of PA-STPA. Several countermeasures had been done to resolve these issue. The unsolved problems were discussed and proposed as further works to refine the proposed PA-STPA.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Systems-theoretic process analysis (STPA) is a new hazard analysis approach based on systems theory and systems thinking. It has capability to identify hazard resulting from dysfunctional component interactions or software problems that frequently present in a complex-automated system (Leveson, 2011). These hazard types cannot be captured by traditional hazard analysis approach such as preliminary hazard analysis (PHA). STPA applications have been demonstrated to several industry such as maritime (Abrecht, 2016; Aps et al., 2017; Rokseth et al., 2017), nuclear (Song, 2012; Thomas et al., 2012; Lee et al., 2013), process (Hardy and Guarnieri, 2011; Rodríguez and Díaz, 2016), oil and gas (Budde, 2012; Hoel, 2012) and subsea (Rachman and Ratnayake, 2015; Zikrullah, 2017).

One major practical challenge has been identified from STPA. The number of produced constraints and loss scenarios are considerably high (Zikrullah, 2017). Logically, the most critical cause of hazard should have more importance. However, there are no distinction of priority between the results of current STPA approach. Considerable amount of results with equal importance makes the decision of resource allocation for problem-solving becomes more difficult.

This problem is not unique only to STPA. Several other tools, such as preliminary hazard analysis (PHA), failure mode effect and criticality analysis (FMECA) and hazard and operability study (HAZOP) also produce considerable amount of results. The only difference is that these other tools already implement prioritization approach in their analysis procedure such as risk matrix, risk priority number (RPN), etc. This prioritization approach increases the efficiency of decision making since the importance between each results is apparent and resources can be allocated accordingly.

STPA is currently only a qualitative analysis approach which focuses on identifying all type of hazards and the possible loss scenarios. Differently, prioritization approach requires quantification of the qualitative values so that it can be compared between each other. Currently, STPA has a gap between the translation of qualitative analysis into quantitative values. Research is required to discover the approach to fill the gap.

A study case is required to demonstrate the application of proposed approach. Subsea systems are type of complex system that benefit with the application of STPA. It is located in deep and harsh underwater environment and have high complexity due to the use of fully-automated system for operation. The proposed approach is to be demonstrated "to the Subsea Gate Box (SGB)" system. It is a new concept currently developed by subsea production and processing (SUBPRO) research center.

1.2 Objectives

The main purpose of this master thesis is to create a framework for prioritization in UCA. The proposed approach is to be demonstrated for a novel technology for subsea processing systems called "the Subsea Gate Box (SGB)". Initial work has been performed to apply STPA to the SGB by Zikrullah (2017). The evaluation of the proposed approach can be performed by comparing the result from both approaches. The objective can be addressed, as presented in the report, into several main tasks listed below:

1. Investigate prioritization approach used in other safety analysis tool
2. Identify useful criteria for prioritization in STPA
3. Propose an approach for prioritization of STPA results
4. Apply the proposed approach to a study case in subsea systems
5. Evaluate the proposed approach

The goal is then to evaluate the applicability and limitation of the proposed method when used in the actual industrial case. STPA is not a specific industry limited method. Different industry with similar characteristic as subsea systems such as nuclear, process industry and oil and gas, may also benefit greatly with the improvement of the methods.

1.3 Delimitations

There are three limitations that is considered when working with the five tasks. First, the proposed STPA approach is developed for analysis of novel design system. During this phase, detailed information about the system is not available yet. Thus, the proposed STPA approach is more suitable for safety analysis with general level information.

Second, developing a completely different approach for prioritization is not the objective of the current research. The author is researching from the available prioritization approaches and only made modifications to tailor those approach for STPA. Thus, advantages and weaknesses of the available approach may be carried over to the proposed STPA approach. However, the focus in this research is rather to make a framework for prioritization in STPA. Thus, the advantages and weaknesses of the proposed approach are presented at the latter section and important points for improvement are mentioned briefly for further work.

A third limitation arises during evaluation of the proposed approach. For the evaluation, a comparison assessment is performed between the result of original STPA analysis and the proposed prioritized STPA approach result. Although the assessment is objective, it is limited only to the outcome produced by the current system used. It is arguable that different system may offer different results which affect the conclusion of the assessment. Therefore, the reader should proceed with caution when using the proposed approach conclusion for their work.

1.4 Approach

The research is divided into two phases. Initially, it starts with desk research to gather relevant literature which serves as foundation knowledge. Relevant literature is analyzed and

discussed further to propose an approach for STPA. Afterwards, a study case of subsea systems is performed with the proposed approach. The findings from the research are evaluated and compared with the initial work from Zikrullah (2017) and summarized into this master thesis.

1.4.1 Literature Survey

The main search engines used to gather literature are either from oria.no, scholar.google.com or sunnyday.mit.edu/STAMP-publications.html. The literature used is only the accessible version from Norges Teknisk-Naturvitenskapelige Universitet (NTNU) library.

First, relevant results of literature study and study case performed initially during the specialization project are summarized and presented. Leveson (2011)'s "Engineering for A Safer World" book is the foundation of the methodology performed in both research. In this book, Leveson starts by questioning the adequacy of traditional causality model. She then developed a new model of causation called Systems-Theoretic Accident Model and Processes (STAMP).

Subsequently, books by Leveson and Thomas (2013); Thomas (2017); Leveson and Thomas (2018) are used as guidelines to describe the procedure of applying the basic STPA. Additional literature by Folse (2017) is used to clarify unclear part of the procedure. He managed to demonstrate an example of systematic and exhaustive STPA report which inspired the author previous work.

Then, detailed explanation of the system used for study case has been gathered from literature by Tjomsland and Lie (2017) and discussions with Postdoc. Arias as the responsible person who develop the subsea gate box concept in SUBPRO. Several simplifications of the system have been made due to limited resource and time. However, the simplifications are still considered as relevant to demonstrate the safety analysis for subsea processing systems during normal operations and specific case of bypass operations.

Afterwards, discussions about available prioritization approach are made. The book by Rausand (2013) is used to describe methodology used in risk analysis. Related prioritization approach from other tools such as PHA, FMECA and HAZOP is discussed further.

The author then gathers relevant prioritization criteria for safety analysis. They are assessed according to their suitability for each step of STPA. The related criteria are then integrated into the proposed modified approach for STPA.

1.4.2 Study Case

The proposed approach is then used to analyze the same subsea system that has been used for initial analysis by Zikrullah (2017). Several modifications and improvements on the approach are performed through the analysis work. The produced prioritized results of STPA are then compared with the basic STPA results for assessment. Two criteria have been defined for the assessment, efficiency and safety. Additionally, discussions on the weaknesses of the proposed approach are also performed to point out the part that needs to be improved.

1.5 Structure of the Report

The thesis is arranged based on the objective in Section 1.2. Chapter one is introducing the background, objective, scope and limitations and the method used in the research.

Chapter two starts with an introduction of STAMP basic theory. Afterwards, a thorough explanation for the new hazard analysis method, called STPA (later called as original STPA for distinction), is presented.

The third chapter is the summary of study case and the results from the initial research by Zikrullah (2017). Selected discussion from the previous work, related to the current research, is presented at the end of the chapter.

The fourth chapter describes the literature study on prioritization. Several approach based on similar safety analysis tools are presented and discussed. It continues with discussion on several useful criteria that can be used for STPA. Thorough assessment of the criteria is then performed. The chapter concludes with a proposed approach called the prioritization approach for STPA (PA-STPA).

The fifth chapter demonstrates the example of PA-STPA for each step of the analysis. Discussions are made at the end of each step based on the findings.

The sixth chapter begins with the evaluation of PA-STPA compared to original STPA. The weaknesses of PA-STPA are discussed further.

Finally, conclusions and recommendations for further work from this report are presented in the epilogue of chapter seven.

Chapter 2

STAMP & STPA

The main purpose of this chapter is to explain about STAMP and STPA. This chapter begins with introduction of accident model. It continues with elaboration on the recently developed accident model based on systems theory and systems thinking which came to be known as STAMP accident model. STPA is a hazard analysis tool based on STAMP accident model that becomes the main focus for development and discussion in the subsequent chapter. Brief description of STPA is presented together with step by step methodology at the end of the chapter.

2.1 Accident Causality Model

An accident causality model (or accident model for short) is explained as model used to explain the underlying connection that leads to accident. It is built based on the assumptions that there are similar patterns leading into accidents, not just due to random events (Leveson, 2011, pg. 15). Countermeasures can be taken to prevent future accidents by identifying and controlling hazards found from the models.

One of the first theory of accident model, date back to the early 1930s, is called the Heinrich's Domino Model. The model illustrates how the process of falling domino represents a chain reaction that leads to an accident. Afterwards, in 1990, Reason proposed a new model called the Swiss Cheese Model. It is based on the graphical depiction that accident is an event that happened like an arrow through the holes in the cheese (failed barriers or defenses). Notwithstanding the differences on illustration, both have similar assumptions where chain of direct and latent causes of events are the main contributor of accident. It is shown clearly from several tools that were developed from the model such as Preliminary Hazard Analysis (PHA), Failure Mode Effect and Criticality Analysis (FMECA), Hazard and Operability study (HAZOP), etc. They are created to analyze possible hazards and prepare countermeasures to prevent accident. The analysis of a system may shown numerous causes that can leads into accidents. However, they have similar characteristic, the causes are mostly due to direct causes. The causes can either be human or mechanical. The improvements that can be performed are either to increase the reliability of human or components or to include another defense in depth barrier to increase systems robustness to failure.

Several accidents like Mars Polar Landing (1998) and Bhopal disaster (1984) proved that the current accident model and analysis might be insufficient. In both event, they identified that direct causes were not the main contributor. For the first event, the problems were due to conflicting requirement of the system, which were not accounted during the design stage (Board and Casani, 2000). On the latter event, the systems initially have worked properly

according to the initial design. However, various interaction stemmed from changed company policy and inherent system design deficiency further increased the system vulnerability (Bogard, 1989). Both examples show that although the chain of events are apparent now, the causal factors were hidden. Factors such as conflicting design requirement and increasing system vulnerability due to system interactions are neglected in the current accident models.

Rasmussen (1997) argues that in order to understand safety and have better accident model, an approach based on systems theory is a necessity. Currently, industry 4.0 system is being developed for various industry. The integration of software intensive systems, to achieve industry 4.0 objective, increases systems complexity. The process of decomposing system into structural elements becomes more difficult, if not impossible. Complex systems may exhibit unique behavior, called emergence, that cannot be inferred just from each component behavior. Systems theory acknowledges system complexity and instead try to look from the relationship and interactions among each component or event to achieve system safety. Leveson (2004) proposed a new accident model based on systems theory, called Systems-Theoretic Accident Model and Processes (STAMP).

2.2 Systems-Theoretic Accident Model and Processes (STAMP)

System-Theoretic Accident Model and Processes (STAMP) is an accident model built based on systems theory. In systems theory, safety is an emergent property (Leveson and Thomas, 2013). Emergent property arises due to connection and interaction between each component in the system. It can be argued that accident, which is the opposite of safety is also an emergent property. Accident can be prevented by prohibiting the set of interactions which considered unsafe and limit the interactions only to a safe interaction which resulted into a safety property.

Contrary to the traditional accident model, STAMP does not focus on prevention of failures, rather STAMP focuses on how to enforce constraints on system behavior. A control action is required to achieved the desirable system states. Based on STAMP causality model, accident happened either due to unsafe control actions that violate the safety constraints or the provided relevant control actions are not followed.

STAMP is built on three pillar concepts which are: safety constraints, hierarchical safety control structure and process models.

2.2.1 Safety Constraints

The first concept of STAMP is safety constraint. Unsuccessful enforcement of the safety constraints may lead into accidents. Safety constraint is a safe system state imposed to the system components during a specific set of conditions. This state can be acquired by controlling the system behavior.

There are two types of control, passive and active controls (Leveson, 2011, pg. 77). Passive controls are something that is built into the systems. It can maintain safety automatically without a need of external intervention such as shield or barriers. Differently, active controls required action to provide protection. It can be achieved typically by implementing a control system.

The required steps to perform an active control are: (1) detection, (2) measurement, (3) interpretation and (4) response. Figure 2.1 shows how it is linked to the control loop. These functions typically need the use of different equipment, such as sensor, controller or actu-

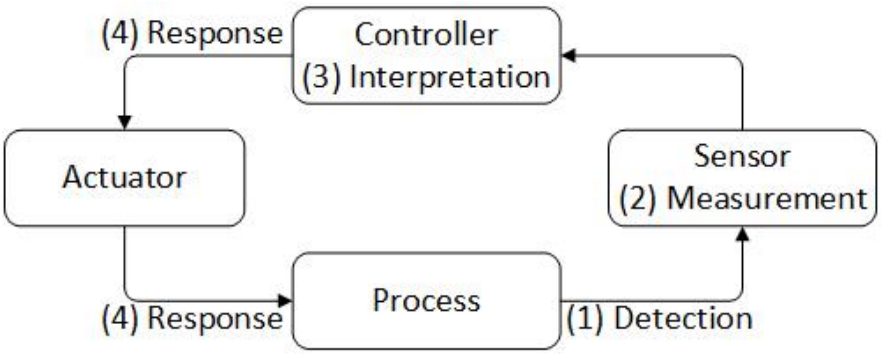


Figure 2.1: Active Control Loop (Folse, 2017)

ator, which in results increased the number of failure modes. The active controls comparatively have higher number of safety constraints than the passive controls.

2.2.2 Hierarchical Safety Control Structure

Hierarchy introduces the concept of elements ranking in the systems relative to each other. This idea becomes the basis of systems theory. The process of thinking starts from the higher level of the hierarchy, with general, low level of details, and refined step by step into the lower level with precise and accurate solution to each elements.

Hierarchical safety control structures, according to STAMP, is a hierarchical structure that illustrates how higher level elements are responsible to enforce safety constraints to the lower level of hierarchy. Accidents happened due to inadequate control action by the controller or due to violation of safety constraints in the behavior of the lower level components (Leveson, 2011, pg. 81).

Each element in the safety control structure communicates in a reciprocal manner. The information from the higher level is used as a reference condition to enforce the safety constraint. The lower level sends a feedback to inform whether the constraints have been satisfied or not.

2.2.3 Process Models

Process model is the third concept of STAMP. A process model is a representation of the system behavior based on several variables and transitions between each state. As seen in Figure 2.1, one of the required steps to perform active control is controller interpretation. The controller needs to compare the information from the feedback with the system process model, shown in Figure 2.2, to determine what sort of control actions are required for the process.

The difficulties of creating a good and efficient process model are dependent to the understanding of the systems and the assumptions made when creating the model. Accidents often occur if there are discrepancies between the process model used by the controller and the actual process (Leveson, 2011, pg. 88). This result into:

1. Provided control is incorrect or unsafe
2. Safe control action is not provided
3. Wrong timing of potentially safe control command (too early or too late)

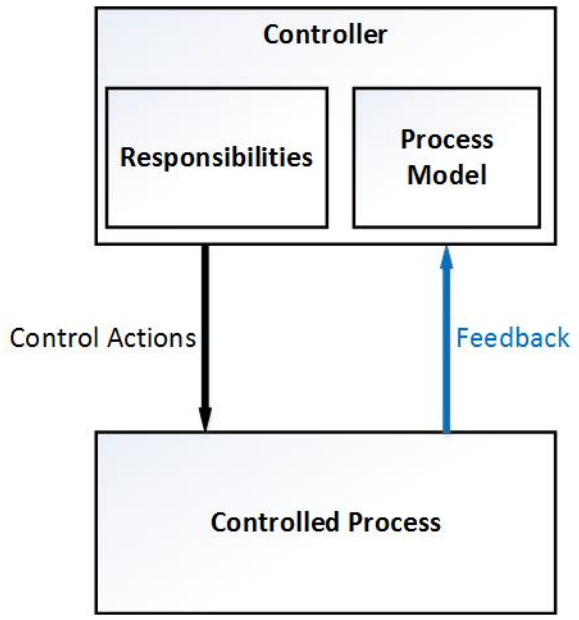


Figure 2.2: Process Model and Responsibilities of the Controller (Leveson and Thomas, 2013)

4. Control is stopped too soon or applied too long

There are two type of actions that can be done by each element in the hierarchy: control actions and provide feedback (see Figure 2.2). Control actions are decisions provided to influence the process or the element at a level below in the hierarchy. Feedback is the information about the reaction of process or element to a command. In hierarchical control structure, both actions might be applied to the same controller. If this situation happened, both inputs serve as variables needed for conditions in the process model.

2.3 Systems-Theoretic Process Analysis (STPA)

Systems-Theoretic Process Analysis (STPA) is a hazard analysis method based on STAMP causality model (Leveson, 2011). STPA has a goal that is to control or eliminate losses through the means of identifying different scenarios based on the identified hazards.

2.3.1 Key Terminologies

Important terminologies used in STPA should be defined first before proceeding with detailed explanation. STPA uses the term loss and scenario similar to other analysis tools. Leveson and Thomas (2018) redefined the terminology of hazard. Additionally, one new terminology is proposed. The new terminology is unsafe control actions (UCAs).

Originally STPA used the term accident. However, since STPA is applicable for different industries, several additional terms are introduced, such as mishap or adverse events. In order to prevent confusion, a more general term, called loss is then adopted as the terminology to be used for unwanted effect of hazard.

> **Definition**: "A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information,

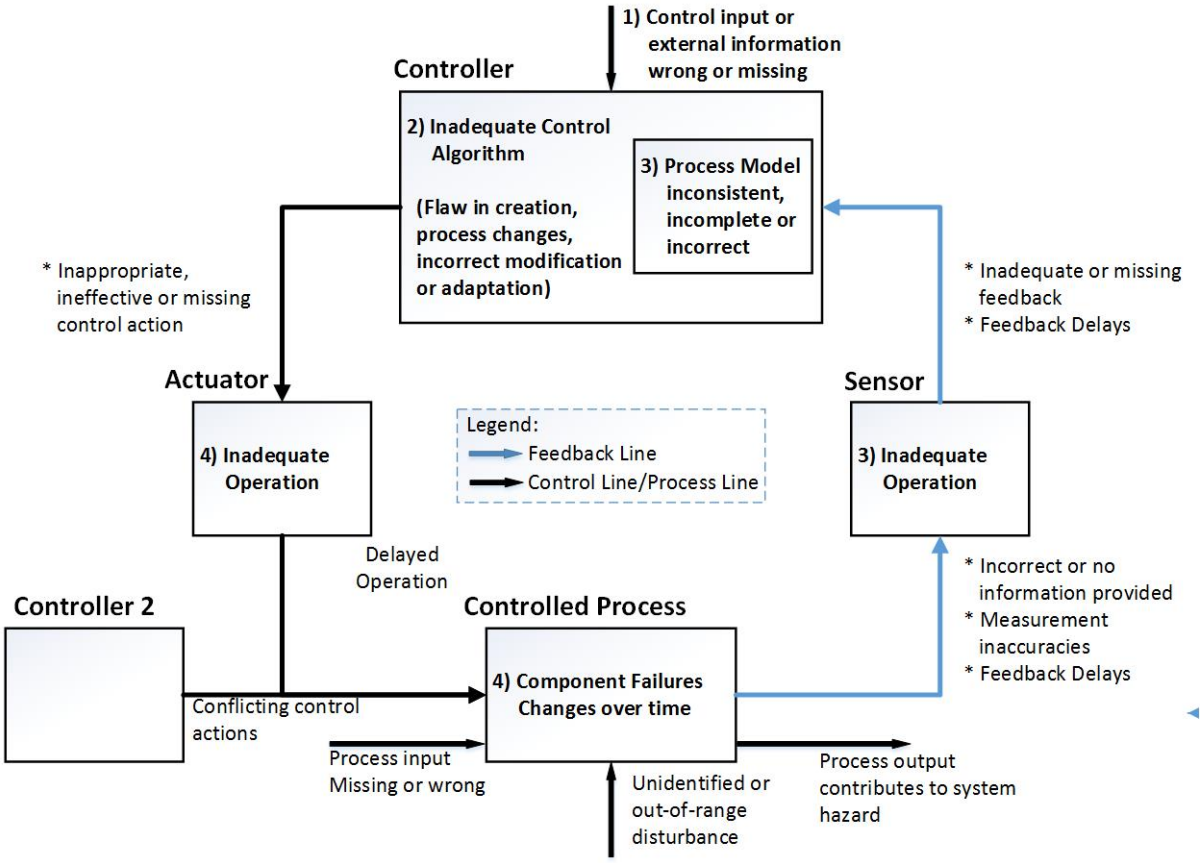


Figure 2.3: Causal factors based on Control Loop Diagram (Leveson and Thomas, 2013)

> or any other loss that is unacceptable to the stakeholders."(Leveson and Thomas, 2018)

Hazard is defined as the initiating point of losses in STPA. There are two important aspects that define a hazard. First, hazard is a system state that is always within the system boundaries of control. Second, hazard can only happen in a system state during a certain set of worst-case condition. The combination of both conditions are required to determine the hazard that want to be avoided. If the system state is always unsafe regardless of the condition, then there is no point to proceed with the analysis and redesign of the system is necessary.

Failure of enforcing safety constraints will then leads into hazards. As mentioned previously, controller are required to provide/not provide control actions to maintain the system behavior. Thus, unsafe control actions (UCAs) can be defined as the inability of controller, either human, mechanical controller or both, to enforce the safety constraints during worst-case set of conditions. There are four types of UCAs:

1. A required control action is not provided to the process
2. A potentially safe control action is provided too late, too early or out of sequence
3. A safe control action is stopped too soon or applied too long
4. An unsafe control action which violated the safety constraints is provided

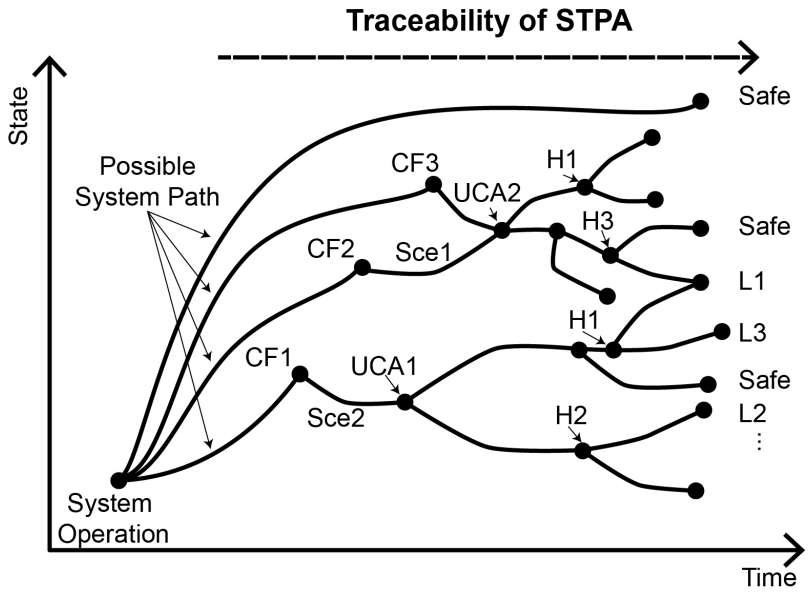


Figure 2.4: Traceability of STPA

Leveson initially tried to illustrate the possible cause of UCA based on the control loop diagram as shown in Figure 2.3. However, this method is unstructured and is people-dependent result scenario based on their comprehension of the system. Leveson and Thomas (2018) developed their model and proposed classification for the cause of loss scenarios into two type:

1. Unsafe control actions occur.
    a. Unsafe controller behavior. This is either due to controller failure, inadequate control logic, unsafe input from other controller or inadequate process model
    b. Causes of inadequate feedback/information. Feedback is either not received or received inadequately.
2. Control actions improperly executed or not executed.
    a. Scenarios involving the control path. Correct control action is given by the controller, but is either not executed or improperly executed
    b. Other factors related to the controlled process. Correct control action is received by the controlled process, but the controlled process either does not execute it or execute it improperly.

STPA process starts from highest level of abstraction by defining the loss and system level hazard. Afterwards, it is refined further into detail elements in the system. This process is called top down approach. The benefit of this approach is that each step can be traced back to the higher level. As shown in Figure 2.4, the causal factor that affects the system, during some sets of environmental conditions may lead into a scenario that trigger an UCA. UCA drive the system into hazardous state which will finally result into either accident or no loss (if mitigation can be enforced).

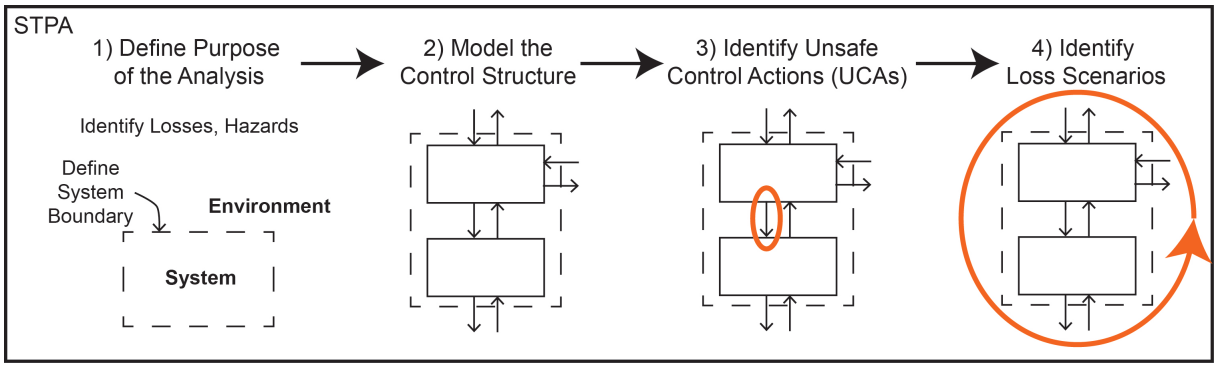


Figure 2.5: Basic STPA Processes (Leveson and Thomas, 2018)

2.3.2 STPA Processes

STPA procedure is initially published on the book "Engineering a Safer World" by Leveson (2011, pg. 211-250). Detailed process of STPA is then explained in the book "An STPA Primer Version 1" with some descriptive examples Leveson and Thomas (2013). Initially, the process of original STPA is split into two steps process, step 1 - identify UCAs and step 2 - identify cause of UCAs. Prior to the analysis, the analysts are required to apply STAMP causality model to define the system engineering foundation. The foundation definition is then considered as step 0 of STPA.

After several years of development and research, Leveson and Thomas (2018) revised the original procedure into a basic STPA process. Two modifications have been made. First, the previously called preparation stage of the original STPA is merged into the method and split into the first two steps of STPA. Thus, basic STPA now has four main steps which is: define purpose of the analysis, model the control structure, identify unsafe control actions (UCAs) and identify loss scenarios. The first modification does not make any changes in the actual process of STPA. An illustration of basic STPA steps can be seen from Figure 2.5.

Second, the safety constraint definition that previously performed after identifying causal scenario is removed. The constraints definition is instead included after UCA definition, which is called as controller constraints. Safety constraints that previously based on system element, other than controller (i.e : sensor, actuator, etc), are combined into controller constraints. The modifications managed to reduce the amount of constraints produced. However, this attempt masks the actual constraint requirement. When the decision maker requires to determine solution for the controller constraints, they still require to look into each scenario and determine the solution, which is basically the original step of STPA.

In this research, basic STPA process has been refined into detail steps to illustrate the flow of work performed. Illustration of the flow of work is separated into 4 flowcharts based on the main step of STPA. The following sections discuss about the detail within each step.

Step 1 - Define Purpose of the Analysis

STPA starts with defining the purpose of the analysis. In this phase, the boundary of the analysis is drawn and relevant documents are prepared for further analysis. Detailed flowchart process during this step can be referred to Figure 2.6.

Step 1.1 Plan and prepare

It is necessary to plan and prepare the analysis carefully to obtain required analysis result. In practice, the approach starts by defining the objective of the analysis. System descrip-

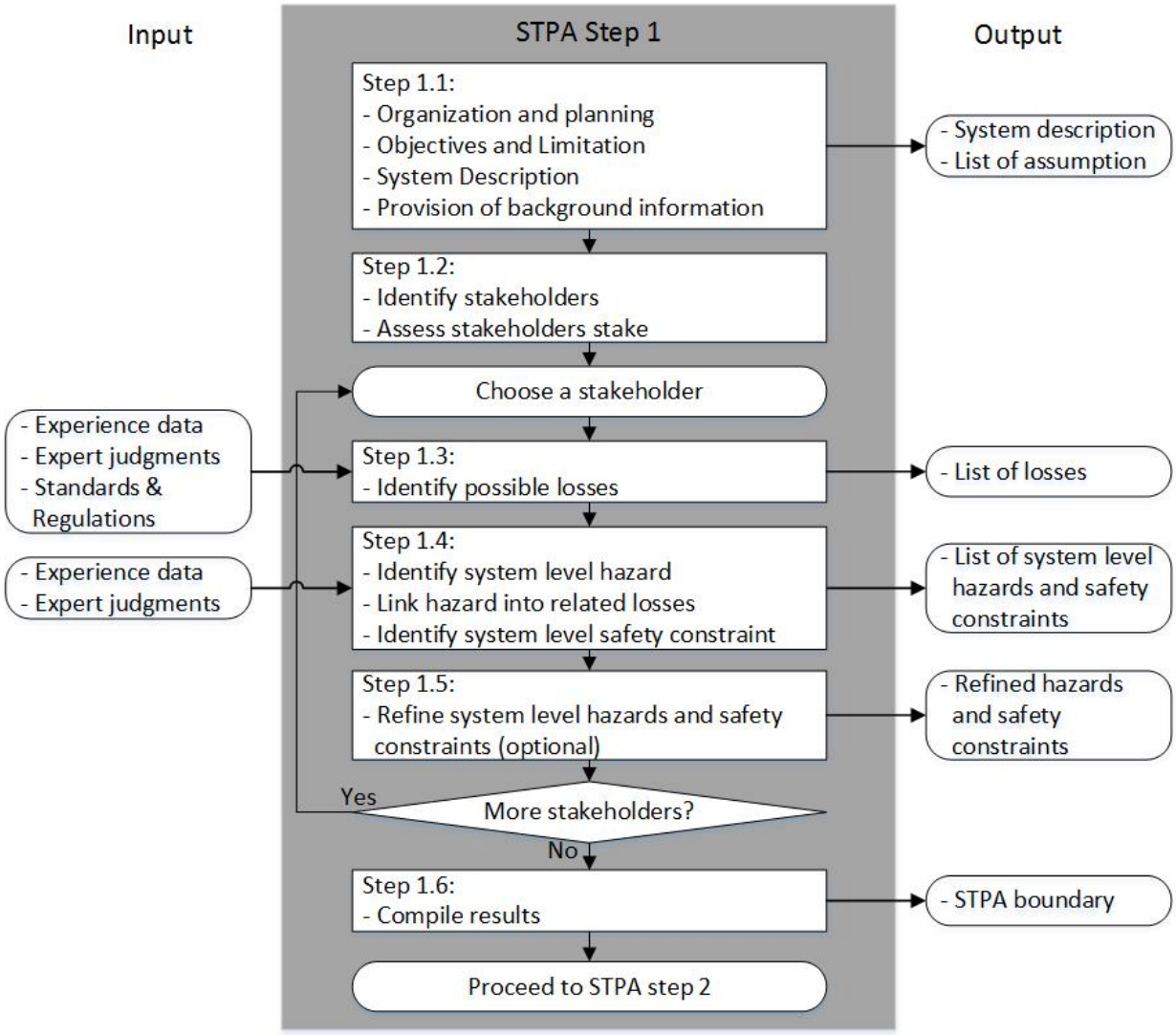


Figure 2.6: Basic STPA Step 1 Flowchart

tion, level of details and acceptance criteria of the analysis are typically obtained during this phase. Afterwards, team member for the study is appointed with one person with the most proficiency of STPA as the team leader (or facilitator as in HAZOP). It is recommended to have experts from different background to make sure that important details are not omitted and to have multiple views during the analysis. Finally, the project plan is specified (including time and resources) to make sure that the analysis is available in due time.

Step 1.2 Identify stakeholders

The next step is to identify stakeholders. Since the hazard analysis is used as an input for decision making, it is important to understand for whom the analysis is prepared. The stakeholders can be management, government, and/or customers.

Step 1.3 Identify losses

Stakeholders may then define the losses that needs to be considered during the analysis. Government authorities typically provide standards to define what can be considered as loss. However, for financial loss and reputation loss, it may differ from one company to another, depending on the company policy. It is mentioned in the handbook of STPA that the loss can

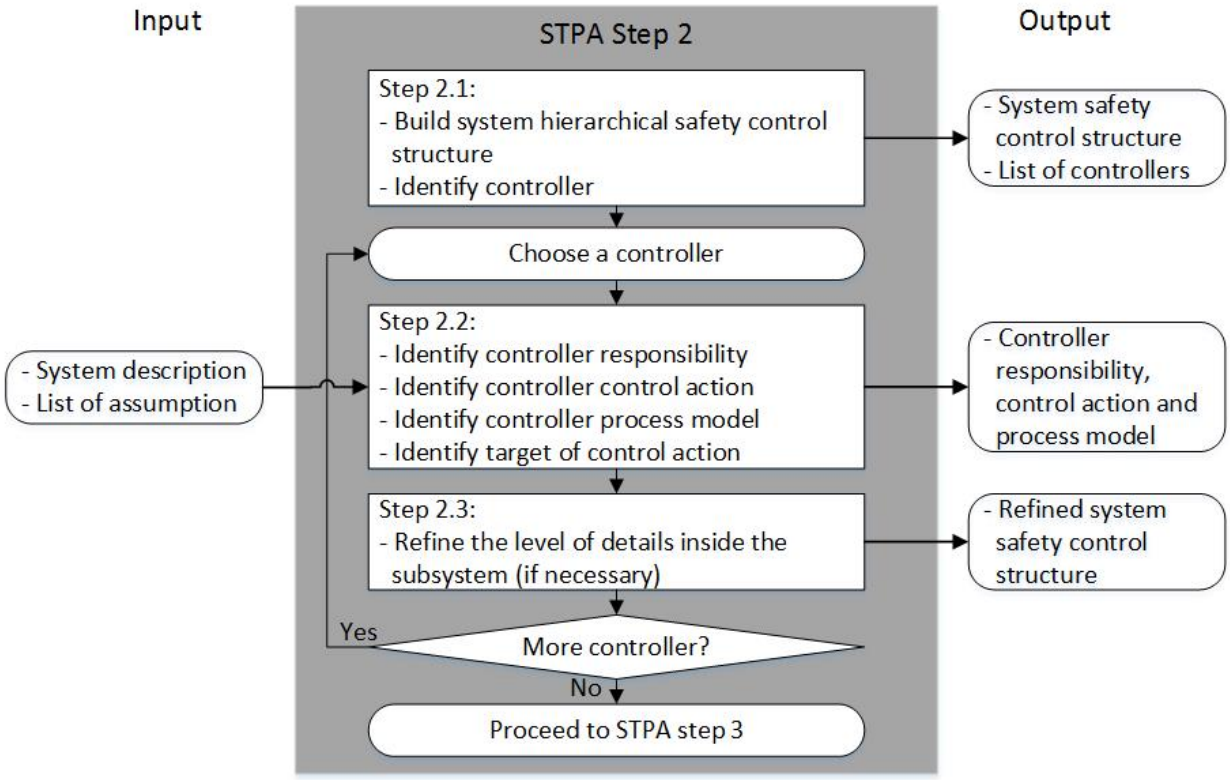


Figure 2.7: Basic STPA Step 2 Flowchart

be ranked and prioritized if there are several losses identified (Leveson and Thomas, 2018). However, no additional explanation about how it can be performed is presented.

Step 1.4 Identify system level hazards and safety constraints

System level hazards and system level safety constraints are identified afterwards. As explained previously, the analyst must consider each system condition and linked it to appropriate worst-case environment condition to determine system level hazard. Each hazard may be linked to one or more loss(es). System level safety constraints are generated by negating the sentence of hazard and paraphrasing it into an imperative sentence.

It is important to note that at this stage, as suggested by Leveson and Thomas (2013), the number of system level hazards to be keep no more than 10. This limitation will help the analyst to start from the higher level of abstractions.

Step 1.5 Refine system level hazards and safety constraints (optional)

The identified hazards and safety constraints may be refined further if additional information is available. The refined hazards are also linked to the appropriate losses.

Step 1.6 Compile results of STPA Step 1

The results are gathered and compiled into one as the analysis boundary. If necessary, the analyst may redo previous related section if additional details are introduced to the system.

Step 2 - Model the Control Structure

STPA step 2 objective is to model the system control structure. Various interactions

within the systems are identified and the responsibility for each element are specified. This step output is to have clear understanding about the behavior and interaction of each part in the systems. Detailed flowchart process during this step can be referred to Figure 2.7.

Step 2.1 Build system hierarchical safety control structure

Analyst is required to draw the system safety control structure. Initially the structure can start from a very high level of structure with minimum level of details. As the analysis process goes, the structure can be refined further. It helps to omit unnecessary analysis from the higher level of hierarchy and focus on the necessary one. This can prevent exponential expansion due to increasing level of details.

Step 2.2 Identify controller information

The next step is to identify controller information and how it may interact with other elements. The outputs are controller responsibility and process model. Controller responsibility is specified according to the subsystem function. The process model, as explained before in section 2.2.3, can be constructed from either the feedback, the control actions or the operational requirements. Each condition need to have specific possible states.

Step 2.3 Refine subsystem level of details (optional)

At the end of this step, the level of details of the hierarchical safety control structure can be refined. Previous steps are repeated to include relevant subsystem that have not been identified previously.

Step 3 - Identify unsafe control actions (UCAs)

The objective of STPA step 3 is to analyze each control action and examine how they can lead to the loss. The step output is unsafe control actions and required safety constraint at the controller level. Detailed flowchart process during this step can be referred to Figure 2.8.

Step 3.1 Check combination that leads into hazard

The next step is to check possible combinations. As mentioned previously, one of the two important aspect of hazard is the worst-case condition. In STPA, the possible combinations between each condition state and/or other controller control actions, if there is any, are checked. The set of conditions are then judged whether they have any possibility to lead into hazard. Depending on the number of states considered, the number of possible combinations may grow exponentially.

There is a systematic methodology created by (Leveson and Thomas, 2013, pg. 66) to make sure that all possible combinations have been identified. They proposes to create a context table. Inside the table, each combination of conditions is systematically checked one by one according to the unsafe control actions that have been defined before. The combinations are then linked to the possible hazard that may occur. An example of a context table can be seen in Table 2.1

Step 3.2 Compile unsafe control actions (UCAs)

Based on the result from context table, the combinations can be compiled into another table called the UCA table as seen in Table 2.2. The table are separated based on each controller loop to distinguish between each other. Each UCA contains several information such as: control actions, unsafe conditions, and link to hazard.

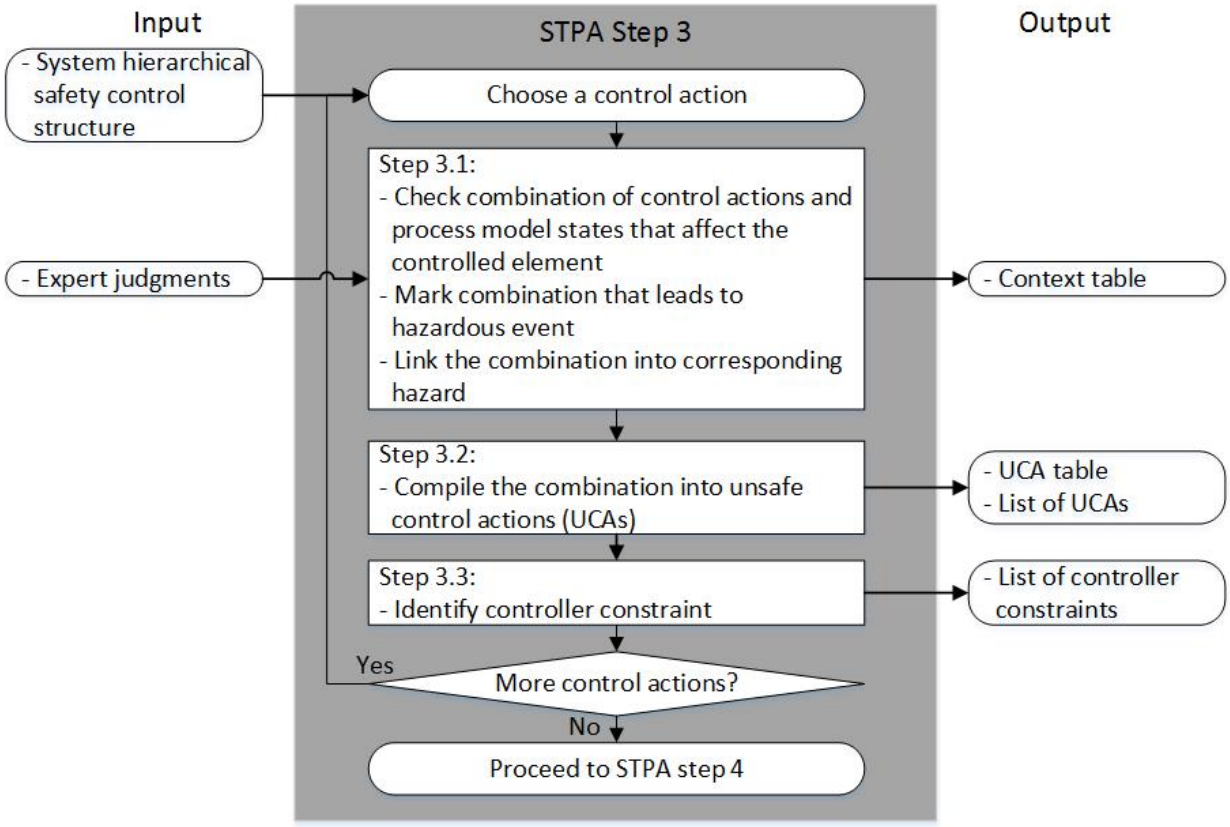


Figure 2.8: Basic STPA Step 3 Flowchart

Control Action	Train Motion	Emergency	Train Position	Hazardous Control Action?		
				If provided any time in this context	If provided too early in this context	If provided too late in this context
Door open command provided	Train is moving	No emergency	(doesn't matter)	Yes (H-2)	Yes (H-2)	Yes (H-2)
Door open command provided	Train is moving	Emergency exists	(doesn't matter)	Yes (H-2)	Yes (H-2)	Yes (H-2)
Door open command provided	Train is stopped	Emergency exists	(doesn't matter)	No	No	Yes (H-3)

Table 2.1: Context Table (Example) (Adapted from (Leveson and Thomas, 2013, pg. 70))

Control Action	Hazardous Control Actions			
	Not Providing Causes Hazard	**Providing Causes Hazard**	**Wrong Timing or Order Causes Hazard**	**Stopped too Soon or Applied too Long**
Open train doors	Door open command not provided when train is stopped at platform and person in doorway [H-1]	Door open command is provided when train is moving and there is no emergency [H-2]	Door open command is provided more than X seconds after train stops during an emergency [H-3]	N/A

Table 2.2: Unsafe Control Actions (UCAs) Table (Example) (Adapted from (Leveson and Thomas, 2013, pg. 72))

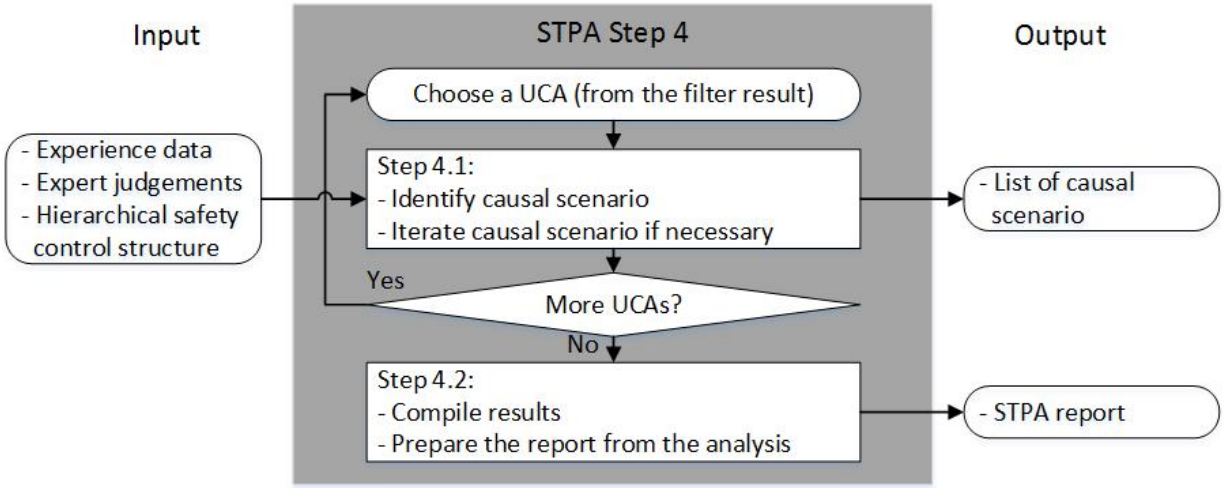


Figure 2.9: Basic STPA Step 4 Flowchart

Step 3.3 Identify controller constraints

Finally, each UCA is paraphrased to create the constraints for each controller. These constraints become the requirement of each controller in performing control actions.

Step 4 - Identify loss scenarios

The final step of STPA objective is to identify possible scenario that lead into loss. STPA analysis originally stop when the scenario is produced. However, the analyst can recommend solution if they are required in the initial objective. Finally, report can be distributed to stakeholders as an input for decision maker. Detailed flowchart process during this step can be referred to Figure 2.9.

Step 4.1 Identify loss causal scenarios

The four types of causal factors, mentioned previously in section 2.3.1, are checked according to each UCA to generate high level scenario. During scenario identification, it is possible to add more detailed elements in the loop in order to specify what is the causal factor of loss.

Step 4.2 Report the analysis

All the results are then compiled into a report. It is important to check whether each

analysis result can be traced back to the previous steps. The complete results are attached and the most important findings shall be discussed. The report should be as clear and as concise as possible to make sure that the decision maker understands and have confidence with the analysis results.

Chapter 3

Systems Theoretic Process Analysis (STPA) of Subsea Gate Box

This chapter purpose is to illustrate the application of basic STPA to a study case in subsea processing systems. The results presented here are used as basis for comparison with the proposed approach results presented in the latter chapter. The chapter starts with introduction of the study case, "Subsea Gate Box". Afterwards, a brief demonstration of how basic STPA was being performed to analyze SGB is presented. Only selected discussion which becomes the rationale on performing current research is presented at the end of the chapter. Complete discussion about the result is not performed, since it is beyond the scope of this chapter. Interested reader may refer to work by Zikrullah (2017) for thorough explanation and discussion about the analysis results.

3.1 Subsea Gate Box

Subsea Production and Processing (SUBPRO) research center, is developing a new field architecture concept to achieve efficient and optimal management of the integrated system over the entire lifetime of the field. Postdoc. Arias was given task to lead the project and currently is performing feasibility study and performance analysis of the system. The assembly of subsea system is called “the Subsea Gate Box”. The subsea gate box (or SGB for short) aimed to provide specialized solution by providing individual processing facility for each well. She found out that the new concept design has three main advantages:

1. SGB can increase recovery of each well
2. SGB ensure that the strong wells are not held back due to constraints posed by the weak well
3. SGB increases the efficiency of separation due to the high pressure of hydrocarbon flowing into the separator

The architecture of SGB is built referring to a lego concept that can be attached and detached depending on the required processing method for each well. An illustration of a subsea gate box with different equipment specified to each well can be seen in Figure 3.1. Individually, it may consist of choke valve, separator, flow meter, multiphase pumps for oil and water and compressor as seen in Figure. 3.2.

[1] Reproduced from Mariana J.C. Diaz Arias presentation (2017)

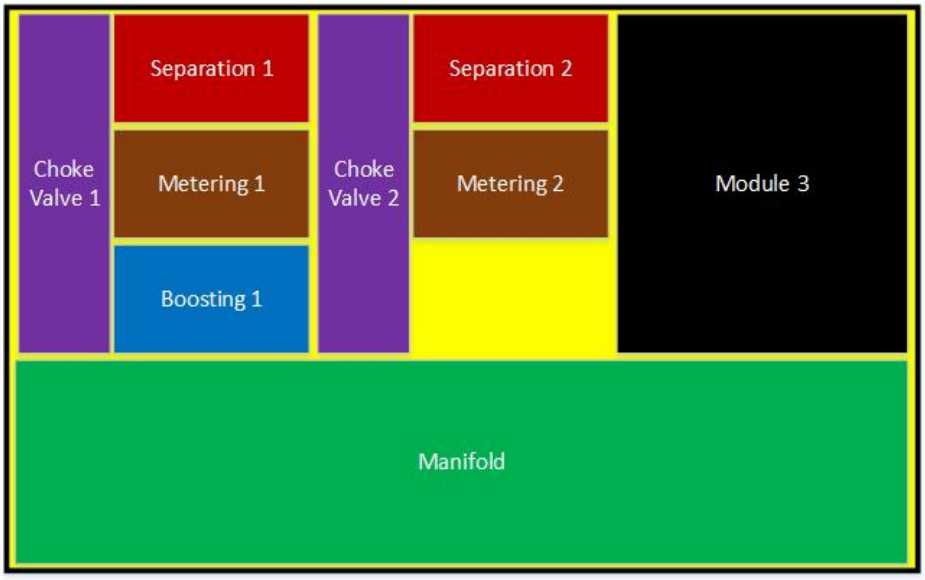


Figure 3.1: Subsea Gate Box Lego Concept [1]

There are two process lines inside the SGB which are designed for normal line and bypass line. For normal process line, hydrocarbons are separated through the three−phase separators into oil, water and gas. Afterwards, it is measured by a metering system to determine what is the production of each fluids. The water and oil are then pumped by using a multiphase pump and the gas is compressed via compressor, both to the topside facility.

The bypass line is used only when the normal process line is not working. The hydrocarbon flows directly through a choke valve to control the pressure and go directly to topside. In this case, the process line works with reduced efficiency due to inadequate processing step of hydrocarbons.

The lego concept of SGB raises the possibility to alternate flow in the process line during failure of one of the SGB. This concept is only applicable if the well is located near to each other so there will be no requirement for additional pump to transmit the hydrocarbons

3.2 Step 1 - Define Purpose of the Analysis

This section explains step 1 of basic STPA for substep 1.1 to 1.5, referring to procedure previously explained in section 2.3.2. The boundary for current analysis was formalized.

3.2.1 System Description

Subsea gate box (SGB) was used for the analysis of STPA. Several assumptions had been made to simplify the analysis but still complex enough to represent the system. An illustration of the process flow diagram of the SGB can seen in Figure 3.3.

In the current study, for normal process line, hydrocarbons were flowing into a separator to be separated into three phases which are oil, water and gas. The oil and water then flowed in parallel and pumped by each individual multiphase (MP) pump to the topside. The gas was assumed to flow naturally without a need of compression. For bypass line, the hydrocarbon was flowing directly through a choke valve to control the pressure and go directly to topside. Connections between each well to either the normal process line or the bypass

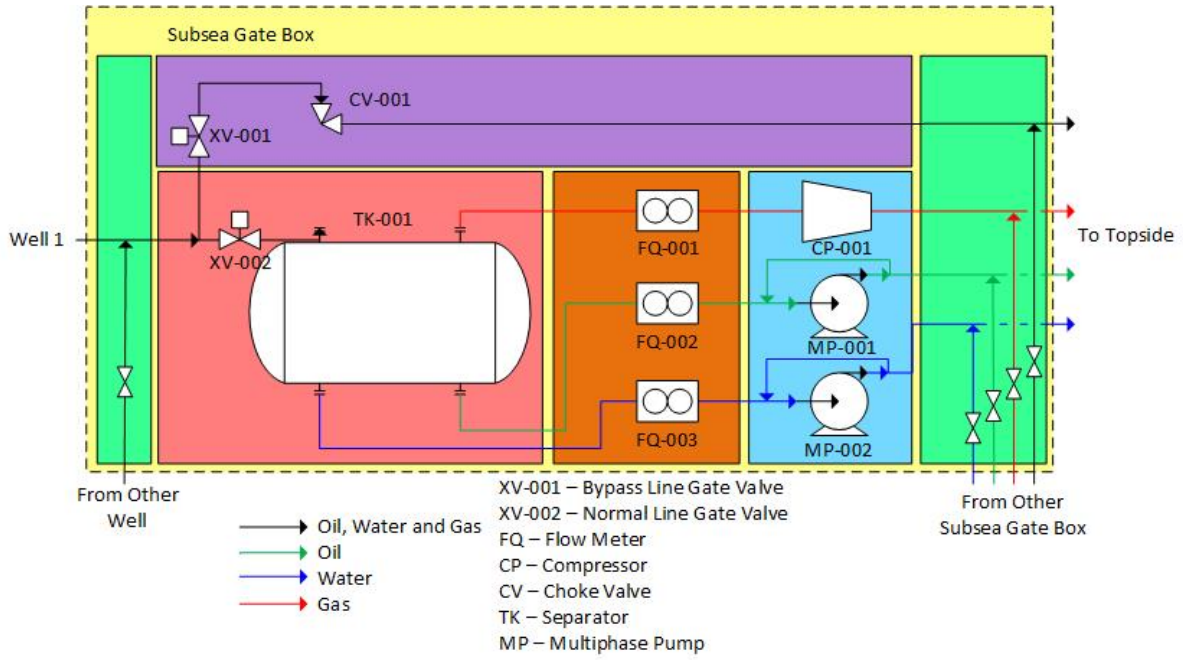


Figure 3.2: Single Subsea Gate Box Process Flow Diagram

process line were controlled manually by the operator via isolation valves.

During normal operation, there were two possible control commands from the operator:

1. Adjust the set point. This control command was applied to choke valve and multiphase pump. It was provided only when there was significant change of pressure in the bypass process line or when there were significant change of pressure differences from the outlet and inlet of the multiphase pump.

2. Bypass process line. This control command was applied only when the normal process line was unavailable. In this case, the flow was rerouted into the bypass line and flowed directly to topside. When the normal process line was available, the flow should return back to the normal process line to increase efficiency.

For this analysis, two similar subsea gate boxes were attached in parallel on one lego structure which were connected via crossover valve. As seen in Figure 3.3, there were possibilities to use either the normal line or the bypass line of the other SGB in case of failure.

3.2.2 Stakeholders and Loss Identification

Four main stakeholders had been identified for the operation of SGB. They were government, company, employee and environmental groups. The government imposed regulation that should be adhered for overall system operation. Company had objective to achieve profit while maintaining their image to the population. Employee was the people responsible with the system operation. Environmental groups had concern with the effect of system operation to the environment.

Three possible events had been identified as unacceptable losses in the process of achieving safety and efficiency in the system operation.

L.1 **Environment pollution.** Release of hydrocarbons to the sea environment.

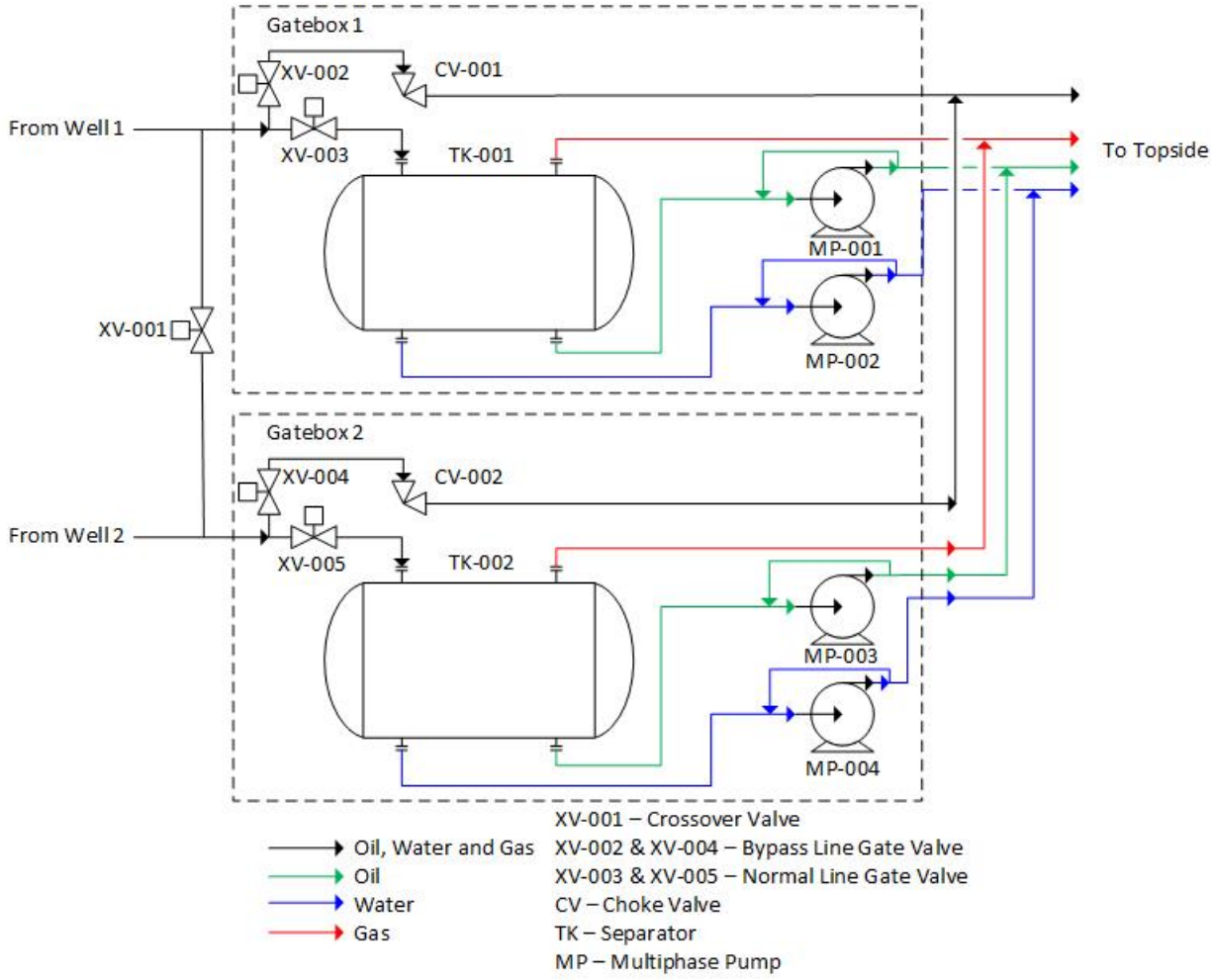


Figure 3.3: Subsea Gate Box for Study Case

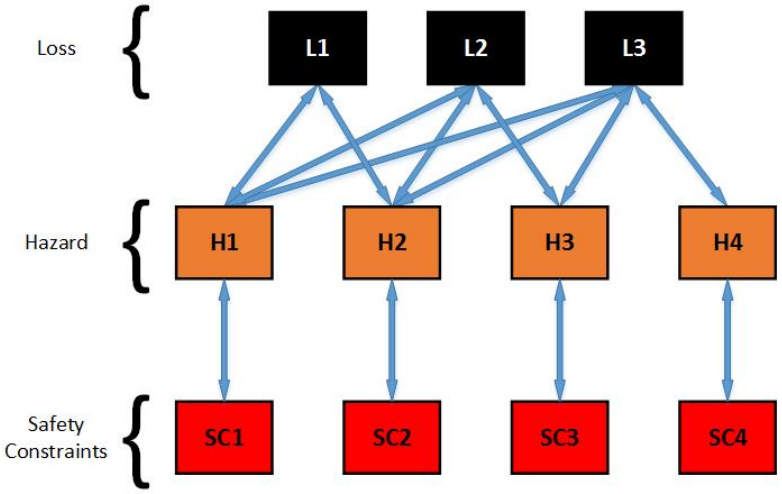


Figure 3.4: Relations Between Losses, Hazards, and Safety Constraints at System Level

Table 3.1: System Level Hazards and Safety Constraints

Hazard	Safety Constraint
H1: Pipeline pressure too high (L1, L2, L3)	SC1: Process line pressure should be maintained properly
H2: Equipment pressure too high (L1, L2, L3)	SC2: Equipment pressure should be appropriate to the process condition
H3: Equipment pressure too low (L2, L3)	SC3: The equipment that need minimum flow should have sufficient pressure
H4: Inefficient hydrocarbon processing (L3)	SC4: The hydrocarbon should be processed with the most optimum option

L.2 **Costly equipment damage.** Subsea Gate Box costly equipment are damaged or destroyed.

L.3 **Unnecessary loss of production.** The production line stops working unnecessarily or working with reduced efficiency.

In case of clashed objective between safety and efficiency, safety had a higher priority for choice. A1: environment pollution had the highest priority due to the harmful effect it could bring to the sea environment and the violation of standard for subsea hydrocarbon processing. A2: costly equipment damage had the second highest priority since the effect was mainly to financial loss. Although it was significant, the costs of cleansing the pollution of hydrocarbons, most of the time, were comparatively greater than the costs of repairing or replacing the equipment. A3: unnecessary loss of production had the lowest priority due to the potential financial loss was lower than the cost of repairing or replacing the equipment. The order of priority could be written as A1 > A2 > A3 based on previous explanation.

3.2.3 System Level Hazards and Safety Constraints

Four possible system level hazards associated with the losses had been identified

H.1 **Pipeline pressure too high (L1, L2, L3)**. Pressure in the pipeline is unable to be controlled by the relevant equipment (e.g: choke valve, pump)

H.2 **Equipment pressure too high (L1, L2, L3)**. Pressure is accumulating inside the equipment without any possibility to flow out.

H.3 **Equipment pressure too low (L2, L3)**. Minimum pressure is violated due to inadequate flow of hydrocarbon

H.4 **Inefficient production process (L3)**. Multiple process line is open at the same time or the setting of hydrocarbon processing is not the most optimum setting.

The hazard can be then rewritten as safety constraints that must be enforced by the designer and operations (see Table 3.1). Each hazard might cause either only one or multiple loss(es). Safety constraints corresponded directly to each hazard. An illustration that represents the connection between loss, hazard and safety constraints on the system level can be seen in Figure 3.4.

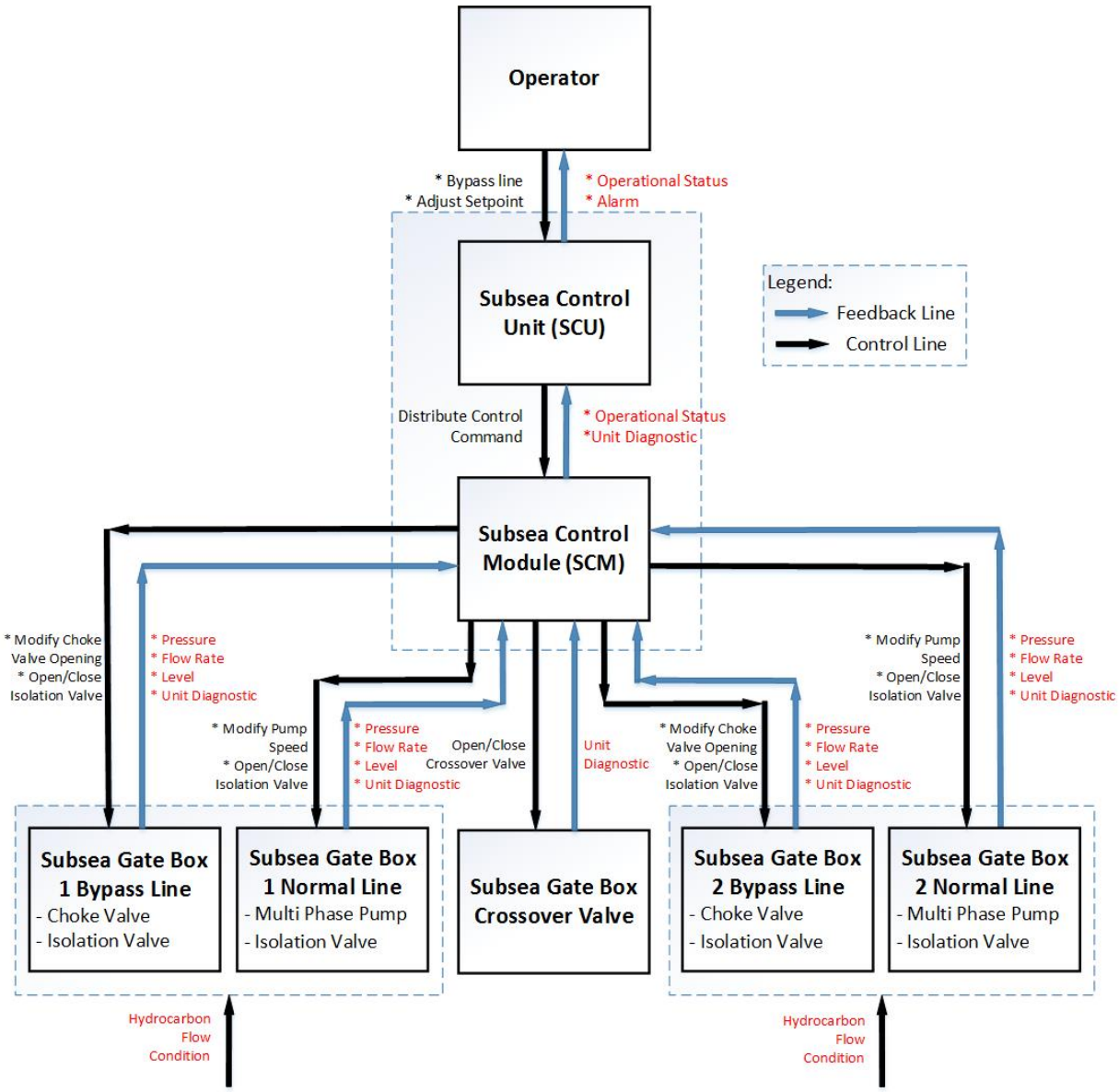


Figure 3.5: Subsea Gate Box Hierarchical Safety Control Structure

3.3 Step 2 - Model the Control Structure

This section explained the step 2 of STPA for substep 2.1 to 2.3, referring to the procedure from section 2.3.2. The hierarchical control structure of SGB is produced and the interconnection between each element in the system is specified.

3.3.1 Hierarchical Safety Control Structure

The system was then modelled into a hierarchical safety control structure as seen in Figure 3.5. The control structure illustrated the elements, interaction and possible control actions and feedback between each element. The black line represented a control command from a controller. The blue line represented a feedback line from the process. This analysis was meant for high level analysis during normal and bypass operation. Several elements that were not related to the current operation, such as shutdown system or have minimal effect to the main control operation, such as passing on the control command or providing

power to actuate the equipment, were not included in the drawing (for example: emergency shutdown (ESD) system, electrical power unit (EPU) and hydraulic power unit (HPU)). These elements could be included later during the analysis for the cause of UCAs (if necessary).

Six elements were defined in the SGB system level hierarchical control structure:

1. Operator. The operator was the main decision maker during the operation of SGB. They had responsibility to determine what type of control actions needed by the SGB depending on the information from operational status and/or process alarm.

2. Subsea Control Unit (SCU). SCU responsibilities were to receive command from the operator and proceed to distribute signals to the appropriate subsea control module. SCU was also responsible to generate alarm and continue the information received from SGB as a feedback to the operator via HMI for decision making.

3. Subsea Control Module (SCM). SCM responsibilities were to receive the command from SCU and proceeded to generate signals to actuate the appropriate SGB equipment. SCM was also responsible to generate alarm and continued the information received from sensor on the SGB processes as a feedback.

4. Subsea Gate Box 1 / 2 Normal Line. It consisted of separator, oil MP pump, water MP pump and normal line isolation valve. The consisting equipment interacted directly with the hydrocarbon process for the normal line and being controlled directly by the controller unit and indirectly by the operator. It was equipped with sensor that give real time status of the process to the controller to be processed.

5. Subsea Gate Box 1 / 2 Bypass Line. It consisted of choke valve and bypass line isolation valve. The consisting equipment interacted directly with the hydrocarbon process for the bypass line and being controlled directly by the controller unit and indirectly by the operator. It was equipped with sensor that give real time status of the process to the controller to be processed.

6. Subsea Gate Box Crossover Valve. It was the equipment that connected the two SGBs. It was only operated during bypass action from the first SGB to the second SGB or vice versa.

Several assumptions had been made in order to proceed with the analysis:

1. Selection Priority. There were priorities in selecting which process line to be used to maximize the efficiency of the system. In case of failure on the normal line of the 1st SGB, the selection priority, from the most preferred to the least preferred, was the 2nd SGB normal line > 1st SGB bypass line > 2nd SGB bypass line if the respective process line is available. In case of failure on the bypass line of the 1st SGB, the selection priority was then 1st SGB normal line > 2nd SGB normal line > 2nd SGB bypass line if the respective process line is available. Any selections differing from those priority order could be considered acceptable but might incur additional loss due to reduced efficiency.

2. Pressure control in the normal line. No pressure control scheme was provided in the normal process line prior to the separator. One of the main advantage of SGB was to have a higher separation rate by utilizing the high pressure from the well. Therefore, the separator itself had been designed to be inherently safe and could withstand maximum calculated pressure from the well.

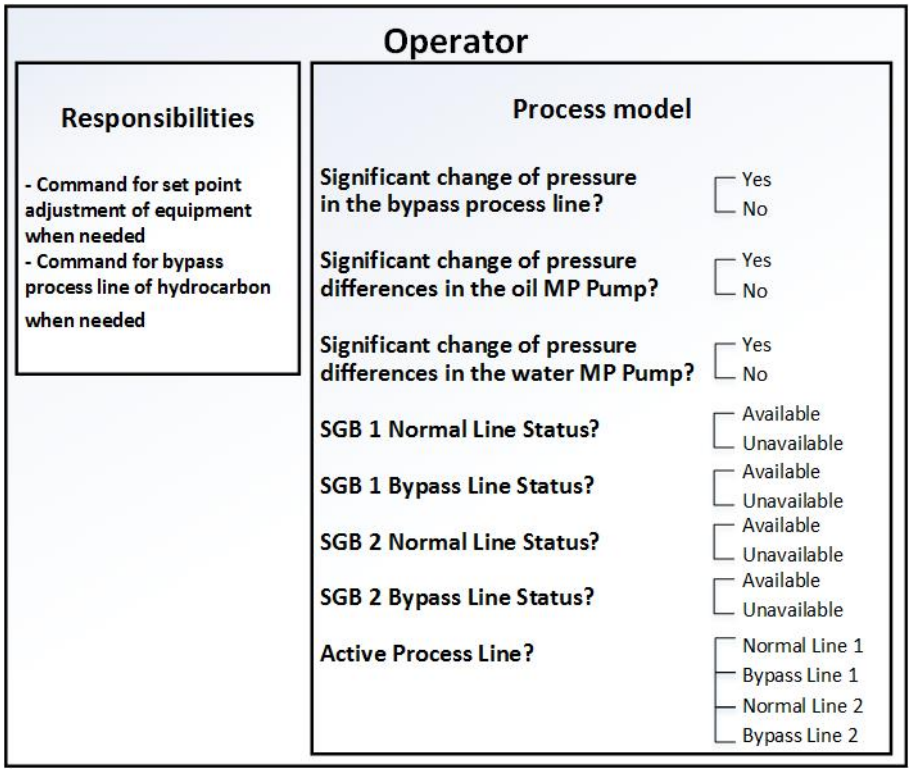


Figure 3.6: Operator Responsibilities and Process Model

3. Controller responsibility. The controller that was responsible to interpret the operator command, either to adjust set point or bypass process line, was the SCM. The SCU was only used to distribute the control action to the appropriate SCM. It was due to the modular design of SGB which allowed single SCM to be used to control the whole SGB. Theoretically, it had the benefit to reduce the memory usage in the SCU and allow faster response of control action.

4. Subsea gate box capacity. The process line was considered to be capable to manage with multiple input from several wells. Therefore the bypass action did not have any requirement to check whether the process line was full or not.

3.3.2 Controller Information

Additional details were then added to the control structure to illustrate how and in what basis did the controllers were working. The controller had a responsibility to perform actions based on each specific process model.

The system safety control hierarchy were divided into three controller loops:

1. Operator − Subsea Control Unit (SCU). An illustration of the operator process model can be seen in Figure 3.6. There were two high level control actions for the operator:

    a. Adjust set point. The control action was provided if there was a need for set point adjustment. Operator needed to judge whether there was flow in the targeted control action to avoid hazard. There were three sub−control actions:

i. Adjust set point of choke valve opening. The control action was provided when the hydrocarbons were flowing in the bypass line and there was significant change of pressure reading in the pipeline.
ii. Adjust set point of oil MP pump speed. The control action was provided when the hydrocarbons were flowing in the normal line and there was a change of pressure differences reading in the oil MP pump.
iii. Adjust set point of water MP pump speed. The control action was provided when the hydrocarbons were flowing in the normal line and there was a change of pressure differences reading in the water MP pump.

b. Bypass process line. The control action was provided if there was a need for rerouting the process line. Operator needed to consider the condition of the designated process line, the current flow route, and whether the option was efficient or not. The control action analyzed here was only the change from SGB1 process line. The change from SGB2 process line was not analyzed due to similar action with the SGB1 process line. There were six sub−control actions:
i. Change flow line from SGB1 normal line to SGB1 bypass line. The control action was provided when the current process was flowing in SGB1 normal line, failures in both SGB1 normal line and SGB2 normal line and normal state in SGB1 bypass line.
ii. Change flow line from SGB1 normal line to SGB2 normal line. The control action was provided when the current process is flowing in SGB1 normal line, failure in SGB1 normal line and normal state in SGB2 normal line.
iii. Change flow line from SGB1 normal line to SGB2 bypass line. The control action was provided when the current process was flowing in SGB1 normal line, failures in SGB1 normal line, SGB1 bypass line and SGB2 normal line and normal state in SGB2 bypass line.
iv. Change flow line from SGB1 bypass line to SGB1 normal line. The control action was provided when the current process was flowing in SGB1 bypass line and normal state in SGB1 normal line.
v. Change flow line from SGB1 bypass line to SGB2 normal line. The control action was provided when the current process was flowing in SGB1 bypass line, failures in both SGB1 bypass line and SGB1 normal line and normal state in SGB2 normal line.
vi. Change flow line from SGB1 bypass line to SGB2 bypass line. The control action was provided when the current process was flowing in SGB1 bypass line, failures in SGB1 bypass line, SGB1 normal line and SGB2 normal line and normal state in SGB2 normal line.

2. Subsea Control Unit (SCU) − Subsea Control Module (SCM). An illustration of the operator process model can be seen in Figure 3.7. There was one control action for the SCU:

a. Distribute control action. The control action was provided when there was a need to distribute control command.

3. Subsea Control Module (SCM) − Subsea Gate Box (SGB 1/2 bypass line, SGB 1/2 normal line, SGB crossover valve). An illustration of the operator process model can be seen in Figure 3.8. There were two high level control actions for the SCM:

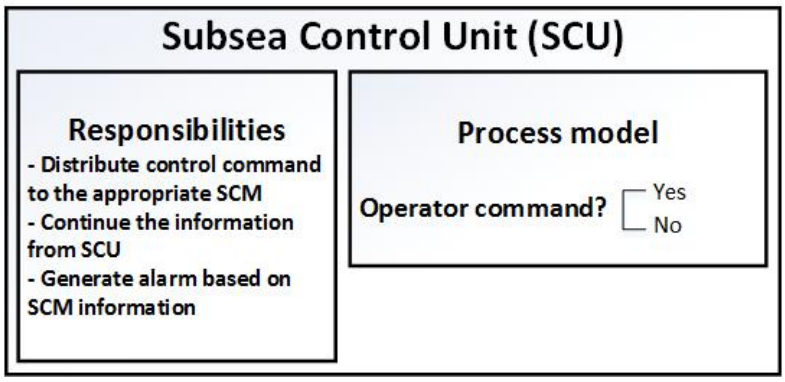


Figure 3.7: SCU Responsibilities and Process Model

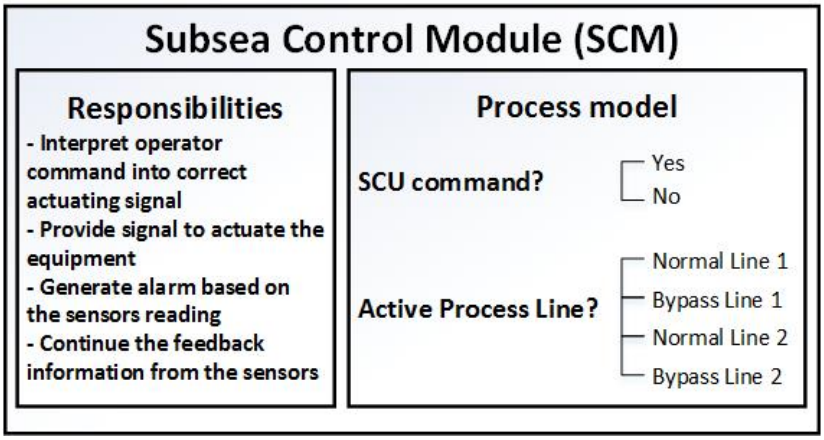


Figure 3.8: SCM Responsibilities and Process Model

a. Implementation of adjust set point. The control was provided when the hydrocarbon was flowing in the correct process line and there was command from SCU to modify the equipment. There were three sub−control actions:
   i. Modify choke valve opening. The control action was provided when the hydrocarbon was flowing in the bypass process line and there was command from SCU to modify the choke valve.
   ii. Modify oil MP pump speed. The control action was provided when the hydrocarbon was flowing in the normal process line and there was command from SCU to modify the oil MP pump speed.
   iii. Modify water MP pump speed. The control action was provided when the hydrocarbon was flowing in the normal process line and there was command from SCU to modify the water MP pump speed.

b. Implementation of bypass operation. The control action was provided when there was command to open / close the respective valve according to the required bypass action. There were six sub− control actions:
   i. Open crossover valve. The control action was provided when the hydrocarbons were flowing in SGB1 process line and there was operator command to change flow line from either SGB1 normal line or SGB1 bypass line to either SGB2 normal line or SGB2 bypass line.
   ii. Close crossover valve. The control action was provided when the hydrocar-

Control Action	Flow In	Hydrocarbon Pressure	Set Point Input	Hazardous Control Action?	
				If provided any time in this context	If not provided in this context
Adjust set point of choke valve	Bypass Line	Significant change	Correct	No	Yes [H1]
Adjust set point of choke valve	Bypass Line	No change	Incorrect	Yes [H1]	No

Table 3.2: Part of Context Table (Loop Operator - SCU)

bons were flowing in SGB2 process line and there was operator command to revert the process line to either SGB1 normal line or SGB1 bypass line.

iii. Open normal line isolation valve (XV−003 / XV−005). The control action was provided when the hydrocarbons were flowing in either SGB1 bypass line, SGB2 normal line and SGB2 bypass line and there was operator command to change the process line to SGB1 normal line. The process model was similar for SGB2 process line.

iv. Close normal line isolation valve (XV−003 / XV−005). The control action was provided when the hydrocarbons were flowing in SGB1 normal line and there was operator command to change the process line to either SGB1 bypass line, SGB2 normal line or SGB2 bypass line. The process model was similar for SGB2 process line.

v. Open bypass line isolation valve (XV−002 / XV−004). The control action was provided when the hydrocarbons were flowing in either SGB1 normal line, SGB2 normal line and SGB2 bypass line and there was operator command to change the process line to SGB1 bypass line. The process model was similar for SGB2 process line.

vi. Close bypass line isolation valve (XV−002 / XV−004). The control action was provided when the hydrocarbons were flowing in either SGB1 bypass line and there was operator command to change the process line to either SGB1 normal line, SGB2 normal line or SGB2 bypass line. The process model was similar for SGB2 process line.

3.4 Step 3 - Identify Unsafe Control Actions

This section explains the step 3 of STPA for substep 3.1 to 3.3 and provides several examples for some of the steps.

The control actions and the process models defined in previous section were then built into a context table, as shown in Table 3.2. An example is taken for the control action "adjust set point of choke valve". It was checked according to the previously defined process model in Section 3.3.2. Additional condition "input set point (correct/incorrect)" was included to check whether the operator were able to respond correctly during each condition and determined whether it was safe or unsafe.

From the context table, the unsafe control actions were then generated into STPA step 1 table. An example is taken from the control action "adjust set point of choke valve" by

Table 3.3: Part of UCA Table (Loop Operator – SCU)

Control Action	Hazardous Control Actions			
	Not Providing Causes Hazard	**Providing Causes Hazard**	**Wrong Timing or Order Causes Hazard**	**Stopped too Soon or Applied too Long**
Adjust Set Point of Choke Valve	... when there is significant change of pressure of hydrocarbon in the SGB bypass line [H1]	... when the set point provided is wrong [H1]	... when applied too late during high pressure of hydrocarbon in the SGB bypass line [H1]	... stopped before the pressure of hydrocarbon in the SGB bypass line return to normal [H1]

operator. Table 3.3 shows the hazardous control actions identified from the selected control action. The related hazard was annotated in brackets. The information from the table was then listed into 4 potential UCAs for the Operator:

UCA.1 The operator does not adjust set point of choke valve when there is significant change of pressure of hydrocarbon in the SGB bypass line [H1]

UCA.2 The operator provides wrong set point of choke valve [H1]

UCA.3 The operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass line [H1]

UCA.4 The operator reverts the set point of choke valve before the pressure of hydrocarbon in the SGB bypass line return to normal [H1]

Based on the UCA, the controller constraints were generated by negating the sentence. The controller constraints were then used as design requirements for the system. The four UCAs identified above then became four controller constraints:

CC.1 The operator must adjust set point of choke valve when there is significant change of pressure of hydrocarbon in the SGB bypass line [H1]

CC.2 The operator must adjust set point of choke valve correctly [H1]

CC.3 The operator must adjust set point of choke valve in time during high pressure of hydrocarbon in the SGB bypass line [H1]

CC.4 The operator must maintain the set point of choke valve until the pressure of hydrocarbon in the SGB bypass line return to normal [H1]

There were 99 UCAs and controller constraints identified in this phase. The complete result of STPA step 3 analysis are presented in Appendix C.

3.5 Step 4 - Identify Loss Scenario

This section demonstrates step 4 of STPA for substep 4.1 and 4.2 and provides several examples as illustration. Every UCAs produced in the previous section were analyzed, based on the previously explained cause of UCA. They were used to determine the possible causal factors and scenarios. An example of analysis for one UCA is presented below

UCA.1 Operator does not adjust set point of choke valve when when there is significant change of pressure of hydrocarbon in the SGB bypass line [H1]

1.A Unsafe controller behavior: Operator understand that there is significant change of pressure of hydrocarbon in the SGB bypass line, but does not provide set point adjustment of choke valve.

1.B Causes of inadequate feedback/information: Operator believes that there is no change of pressure of hydrocarbon in the SGB bypass line, but it is not.

2.A Scenarios involving control path: Operator gives command to adjust set point of choke valve, but the command is not received by the SCU.

2.B Other factor related to the controlled process: SCU receives the command to adjust set point of choke valve, but it is not followed.

Scenario 2.A had clear and concise cause. No additional refinement is needed. Scenario 1.A, 1.B and 2.B were still too abstract. Further analysis was required to unravel the cause of each scenario. The refinement results were presented below.

UCA.1 Operator does not adjust set point of choke valve when there is significant change of pressure of hydrocarbon in the SGB bypass line [H1]

1.A Unsafe controller behavior: Operator understand that there is significant change of pressure of hydrocarbon in the SGB bypass line, but does not provide set point adjustment of choke valve.

i. Refinement: Lack of understanding to the appropriate respond when facing the situation.

1.B Causes of inadequate feedback/information: Operator believes that there is no change of pressure of hydrocarbon in the SGB bypass line, but it is not.

i. Refinement 1: Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.

ii. Refinement 2: Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.

iii. Refinement 3: Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in the SCU.

2.A Scenarios involving control path: Operator gives command to adjust set point of choke valve, but the command is not received by the SCU.

2.B Other factor related to the controlled process: SCU receives the command to adjust set point of choke valve, but it is not followed.

i. Refinement: The command is not followed due to failure in the SCU to generate correct action.

The analysis could be stopped once each scenario clearly stated the causal factor that cause UCA. There were 593 causal scenarios derived from 99 UCAs during normal and bypass operation. Out of 593 scenarios, 171 of them were unrefined scenarios. The actual loss scenarios produced were 422. The complete list of loss scenarios from STPA step 4 analysis can be seen in Appendix .C.

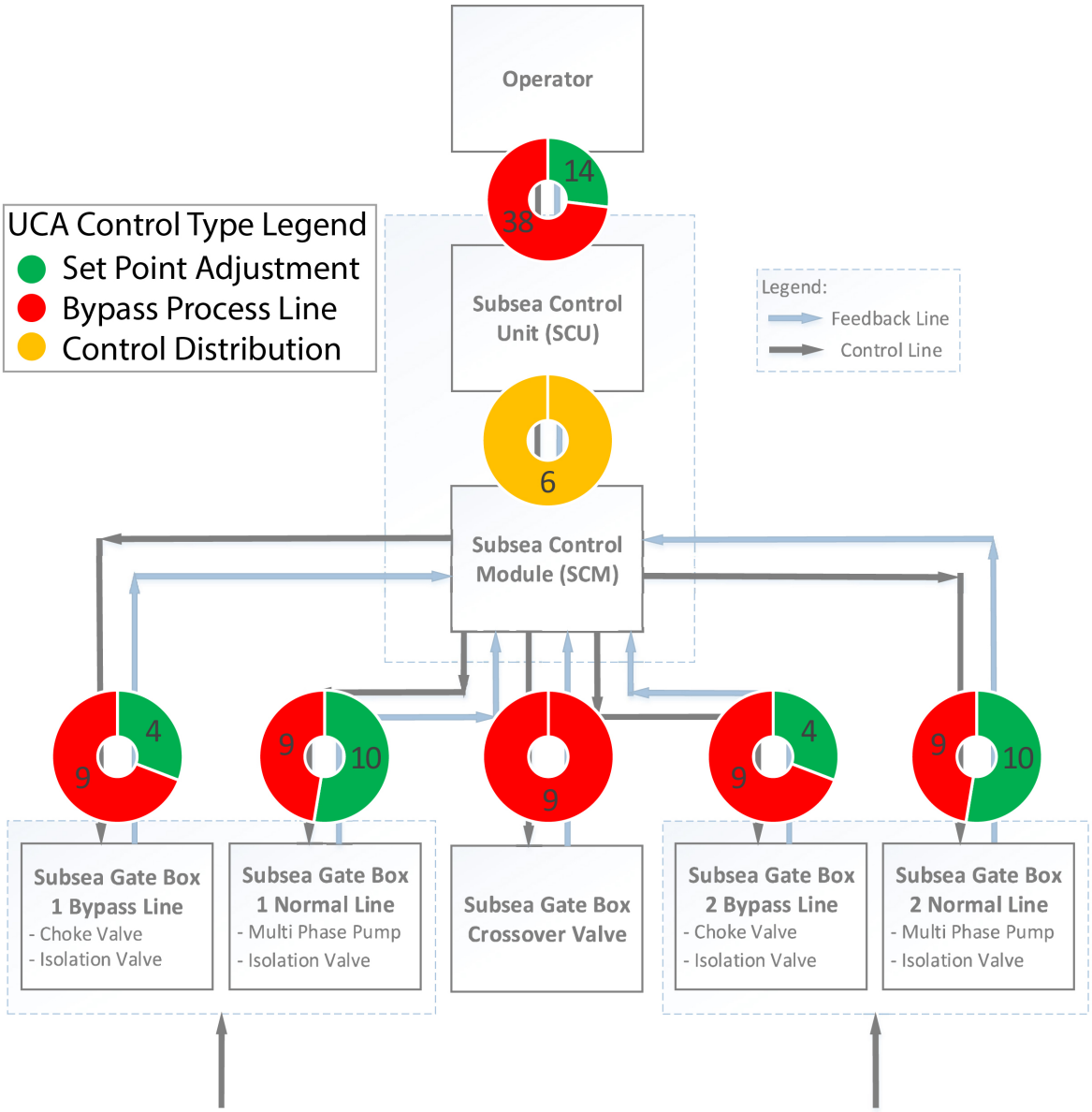


Figure 3.9: UCA Distribution

3.6 Discussion on Prioritization Issue

One of the purpose of hazard and risk analysis, according to IEC61508:2010, is to provide the risk level of hazard. This requirement is to specify which hazard is the most dangerous and should be prioritized to be reduced further into a reasonable level. This state are defined as "as low as reasonably practicable", a term commonly used in risk analysis. It is used to define the state where risk of a system cannot be reduced further due to the unnecessary increase of costs that disproportionate with the benefit gained. However, STPA does not provides such means in the process. It is shown clearly from the long list of results produced by the assessment made the problem-solving management seems endless. Current results of STPA for the SGB managed to produced 99 UCA and 422 scenarios.

There were two simple approaches for prioritization performed in the initial research, which were drawing UCA distribution and constructing the pareto chart of causal factors. Figure 3.9 and 3.10 present the results of these two simple prioritization approaches.

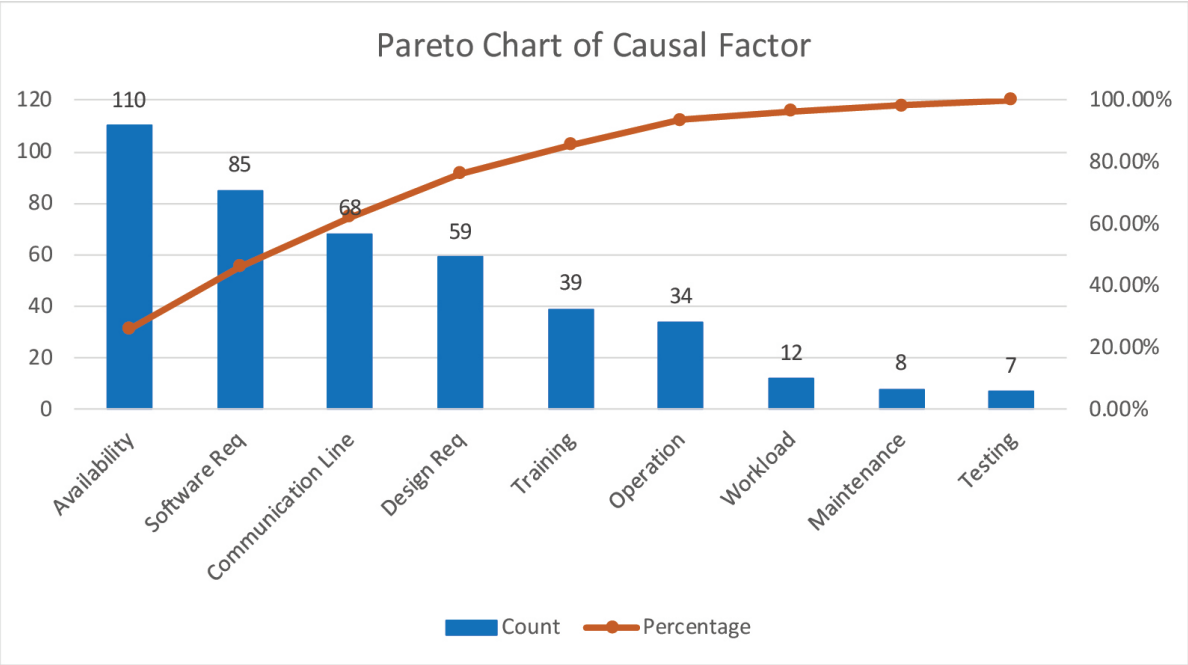


Figure 3.10: Pareto Chart of Causal Factors

From the first approach, the decision maker had to determine which controller have the highest possible number of UCA and rank the controller criticality based on them. However, it was arguable whether the designated controller was truly critical or not. Figure 3.9 shows that operator contributed to higher number of UCA compared to other elements. From the approach, it indicated that larger resources and times should be allocated to reduce the possibility of UCAs due to operator control. However, if more detailed view was taken, then the weakness of the approach became apparent. For example, UCA "Operator does not adjust set point of choke valve when the pressure of hydrocarbon in the SGB bypass line is high [H1]" and "Operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass line [H1]". For this approach, both UCAs should be treated equally since they caused by the same controller. However, simple logical reasoning could be made to judge that the second UCA should have higher priority than the first UCA. This was due to the addition of word "too late" in the second UCA. Therefore, the resource and time should be allocated more for the second UCA.

The pareto chart illustrated the contribution of each type of causal factors. Additionally, it was organized from the highest to the lowest contribution. This attempt managed to shift the focus of causal factors into the five most important factor that contributed to 80% of the problem. However, it was arguable whether these factors have similar importance between each other. Due to the crude attempt when classifying the causal factor, the pareto chart result itself was inaccurate. For example, availability class consisted of SCU failure, choke valve failure, sensor failure, etc. Compared to the operation class, it only consisted of operator mistake and task procedure. The number of causal factor inside each class was different due to unequal distribution. Therefore, it was obvious that availability will always has the highest contribution since it consisted of more causal factor than other class.

These two problems in the initial approaches left a deep mark in the author mind. Despite their limitation, attempts to perform prioritization had been performed and seemed to improve the ease of judgment for decision making. Additionally, when resource and time are limited, they would not be able to solve large number of UCAs and scenarios problem effi-

ciently. Therefore, another approach was required and needed to be tested to accommodate the prioritization issue on STPA.

Chapter 4

New Approach for Risk-Based Decision Making with STPA

The main purpose of this chapter is to introduce and explain the modified STPA. The first part of the chapter defines and elaborates on the concept of risk and risk-based approaches and why these are relevant in the context of STPA. The discussion forms the basis for proposing criteria for risk-based decision making, like prioritization, to be integrated in STPA. The proposed criteria were then assessed against each step of STPA to determine the relevance for use in the proposed method. Finally, proposed modification approach for STPA is explained at the end of the section.

4.1 Risk - What and Why?

In this section, there are two questions that should be asked. First, what is risk? Second, why is risk an important issue to include in our analysis? The two questions can be answered one by one.

First, according to SRA (2015), risk is *the consequences of the activity and associated uncertainties*. The discussion of risk always covers possible event that can happen in the future. When talking about risk, three set of questions are given (Kaplan and Garrick, 1981): *what can go wrong?, what is the likelihood?* and *what are the consequences?*. The answers to these questions can be summarized into a set of triplets (s_i, p_i, c_i), where s_i is scenario, p_i is probability/likelihood and c_i is consequence.

After having basic understanding of risk, the next step is to discover the reason of including risk in our analysis. In order to achieve system safety, systematic approaches have been developed. Hafver et al. (2017) tries to classify the current approaches into two types: risk-based safety philosophy and control-based safety philosophy. In risk-based safety philosophy, safety is achieved by minimizing the risk. On the other hand, control-based safety philosophy consider that safety can be achieved by controlling the system state to be within the safety constraints.

Systematic process based on risk-based safety philosophy has been defined. It is simply described by performing risk assessment consisting of risk analysis and risk evaluation. This approach has been widely accepted in the industry and also included as requirement in standards such as ISO17776 (2002) and ISO31000 (2009). The advantage of this philosophy is that comparison and prioritization of risk can be performed (Hafver et al., 2017). Some examples of tools based on risk-based safety philosophy are PHA, FMECA and HAZOP.

For control-based safety philosophy, control actions are required to prevent system state

move into dangerous state. Some tools based on control-based safety philosophy are STPA and functional resonance analysis method (FRAM). Ideally, the objective of the analysis is to identify all possible loss scenario and to define safety constraints that need to be followed. It has capability to cover various causal factors of accident other than human error and component failures such as interaction problems. However, in reality this feat is difficult to be achieved completely. Controlling the system based on all possible scenarios can incur additional cost and it is not perfectly reliable either (Hafver et al., 2017). Additionally, for complex systems, where the philosophy is originally developed for (Hollnagel and Goteman, 2004; Leveson, 2011), it has characteristic of being difficult to control (Hafver et al., 2017). Therefore, having numerous safety constraints and control strategies do not imply directly that the systems are working safely. This issue raises another question about whether a complete and exhaustive analysis is truly required. If the trade-off between cost and resources to achieve more safety are beneficial, then using the control-based safety philosophy approach is recommended. However, if the trade-off is meaningless or rather harmful, then comparison and prioritization become necessary. This is where the advantage of risk-based safety philosophy is used. Both control-based and risk-based safety philosophies should be used as complimentary approaches to manage safety (Hafver et al., 2017).

4.2 Approaches for Risk Prioritization

An explanation about how prioritization can be performed within risk-based safety philosophy context should be presented before going into details on how to combine both control-based and risk-based safety philosophy. Prioritization comes from the word prioritize, which means *to list or rate (projects, goals, etc.) in order of priority* (Merriam-Webster, 2018). Prioritization is an answer for decision maker's question about the relative importance of things. It is performed by introducing several relevant criteria that are used for assessments. Afterwards, the subjects are either ranked or screened, depending on the requirements, then listed in order. Finally, the prioritized list is presented to decision maker for final choice.

In the world of risk and safety, prioritization is performed during the risk assessment process. The objective is to determine the event with higher risk and prioritize resources allocation to the most important part. As mentioned previously, risk assessment consists of risk analysis and risk evaluation. Risk analysis is a systematic process to analyze risk. Risk evaluation is the assessment of risk against the acceptance criteria to produce the prioritized risk results.

Risk analysis can be classified into three types based on the objective (Rausand, 2013, pg. 121):

1. *Qualitative risk analysis.* In this process, descriptive words are used to describe the scales of hazardous events, frequency and consequences. It is used typically during early stage of the analysis where good quality data is unavailable.

2. *Semi-quantitative risk analysis.* Similar to qualitative risk analysis, the descriptive scales are then given values. Although the scales does not accurately represent the actual magnitude of frequency and consequences, it can still be used to depict risk picture of the system. Some of the approaches are risk matrix and risk priority number (RPN)

3. *Quantitative risk analysis.* The process starts by assigning numerical values to frequency and consequence of the scenario. The numbers are typically gathered from

Table 4.1: Risk Matrix

Frequency \ Severity	1. Improbable	2. Remote	3. Possible	4. Occasional	5. Fairly Normal
5. Catastrophic	5	10	15	20	25
4. Severe Loss	4	8	12	16	20
3. Major Damage	3	6	9	12	15
2. Damage	2	4	6	8	10
1. Minor Damage	1	2	3	4	5

Not acceptable - requires risk reduction measures
Acceptable - consider for further analysis
Acceptable

historical data of the event. Some of the approaches are probabilistic risk analysis (PRA) and probabilistic safety analysis (PSA)

There are two approach when utilizing the prioritized risk assessment results for decision making, which are risk-based decision making (RBDM) and risk-informed decision making (RIDM). RBDM refers to the process where only results of risk assessment, such as quantification of risk, costs and benefits, become the basis for decision making (Johansen, 2010; Rausand, 2013). In this case, some predefined requirements and important measures are used for prioritization. In RIDM, the results of risk assessment are considered together with other relevant measures, such as traditional engineering principle, in order to do the decision making process (Johansen, 2010). Both terms are sometimes used interchangeably by the stakeholders, making the understanding about the role of risk assessment becomes complicated. Therefore, in risk assessment process, the most important starting point is to define what is the basis for decision making together with clarification about the purpose of risk assessment.

Consideration have been made when selecting the relevant approach for risk prioritization. It is impossible to incorporate all approaches for prioritizing risk due to the numerous and diverse amount of available approaches. Thus, constraint should be defined. The main constraint in the current research is the approach should be capable for analysis of novel system development. At this stage, complete information about the system are not available yet, thus reducing the possibility of using pure quantitative approach. However, logical and reasonable results of prioritization are necessary, which also reduces the possibility of using pure qualitative approach.

Semi-quantitative approaches are considered as the most relevant approach in the current research. Several semi-quantitative approaches have been defined in order to evaluate and prioritized system risk based on risk-based safety philosophy. The following subsections are discussing about the related approach.

4.2.1 Risk Matrix

Risk matrix is a table of frequency and severity level of the hazardous events or loss scenarios. The hazardous events are initially gathered from hazard identification and analysis process, such as PHA. The risk matrix can be used to rank, screen and evaluate the hazardous events. In the table, the frequency and severity criteria can be divided into several classes of different magnitude depending on the analyst preference. Example of criteria classification are

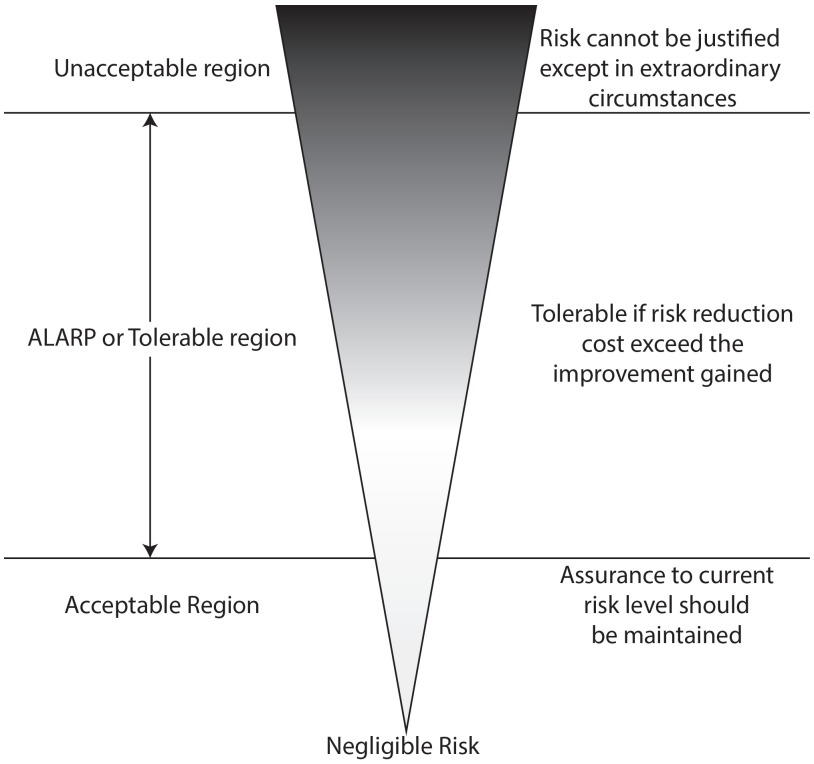


Figure 4.1: The ALARP Principle (Rausand, 2013)

presented latter in the section 4.3.1 and 4.3.2. An illustration of 5x5 risk matrix is presented in Table 4.1.

In the cross section table, some numbers are inserted. They are gained by multiplying the probability (or frequency) of the event (the left most column) by the consequences of the event (the top row), $R = S \times F$, to get the risk of individual hazardous event. An acceptance range is then formed to classify the risk and determine what should be done next.

The risk matrix have several advantages and limitations (Rausand, 2013, pg. 104). First, risk matrix is easy to use and understand. It also has a long track record of use in the risk domain. Additionally, it can be combined with other approaches, such as risk acceptance and risk priority number to get the desired output. However, risk matrix does not have standardize format. it is difficult to determine whether the result of one analysis is comparable to another analysis result, even though similar approach on similar system is used. The risk matrix is also limited by the precursor approach capability to identify hazard. It can only analyze the result gained from previous analysis.

4.2.2 Risk Acceptance Criteria

Prior to risk analysis, a risk acceptance criteria should be established. It is also stated in the standard NS5814 (2008) that *the results of risk analysis must be compared with the criteria for acceptable risk*. The goal is to achieve acceptable risk based on context and current values of society and enterprise (Rausand, 2013, pg. 106).

Several relevant approaches have been developed for risk acceptance. Please note that the list does not cover all existing approaches. It only cover relevant approaches for semi-quantitative risk acceptance criteria:

- *The As Low As Reasonably Practicable (ALARP) Principle.* The risk is divided into three regions which are unacceptable region, ALARP region and broadly acceptable region. An illustration of the ALARP principle can be seen in Figure 4.1. When the risk lays in the ALARP region, a cost benefit analysis is performed to determine whether the cost of implementing solutions proportionate to the risk reduction achieved. It should be continuously performed until the risk becomes negligible and the cost becomes unreasonable to be effective.

- *The As Low As Reasonably Achievable (ALARA) Principle.* Similar to the ALARP principle, the risk should be reduced as long as it is reasonable. However, the ALARA principle does not have broad acceptable region.

- *The Globalement Au Moins Aussi Bon (GAMAB) Principle.* It is a French expression of "globally at least as good". In this principle, the risk of system is compared to similar system where the solution has been implemented. The goal is to have a new system with risk level that at least globally as low as the existing equivalent system.

4.2.3 Risk Priority Number (RPN)

The risk priority number (RPN) is initially developed as part of FMEA/FMECA. It is a ranking and prioritizing approach that is used to assess the design risk based on potential failure modes (J1739, 1994). Three criteria have been established which are severity (S), occurrence (O) and detectability (D). It is classify into 10 classes, from 1 to 10 with different magnitude and range between each class. The ranking factor are then multiplied to give the $RPN = S \times O \times D$. RPN will have result in range from 1 to 1000 with higher numbers denote as having higher risk.

Although RPN is relatively easy to understand and have been widely used currently in industrial practice, it suffers numerous criticisms for its practice. There are several weakness identified in RPN such as the use of ordinal measurement for calculation, uneven distribution of number in the scale, duplicate RPN with different characteristics, and varying sensitivity to small changes in the calculations (Bowles, 2003). Readers who are interested with more thorough discussion of the weaknesses of RPN, shall refer to research paper by Bowles (2003) and Wheeler (2011).

The first weakness of RPN needs to be highlighted since it is the most distinguishable weakness in the approach. In RPN, a scale needs to be defined to measure and classify each criteria. There are four types of known measurements scales (Reaves, 1992): nominal measurement, ordinal measurement, equal interval measurement and ratio measurement. Nominal measurements refer to the use of tag name to distinguish difference between objects. Object classified under the same categories can be counted together and used as frequency data. Ordinal measurements refer to the placement order of things. The scale can use nominal or alphabetical value in sequence. Although the contrast between each part can be distinguished, the disparity in each part can be vague. Equal interval measurements is similar to ordinal measurement but with additional improvement. In this scale, the distance between each place is properly specified and is equal anywhere within the range. Thus, a process of addition and subtraction becomes logical. Finally, the ratio measurements are an equal interval measurements with an improvement. In this scale, absolute zero exists as the lowest reference point. Thus, a process of multiplication and division becomes available in this phase.

Table 4.2: Assessment Result for Criteria

STPA Step	Criteria Assessment					
	Severity	Likelihood	Mitigation	Cost	Effectiveness	Level of Knowledge
Step 1 - Define purpose of the analysis	√	×	×	×	×	√
Step 2 - Model the control structure	×	×	×	×	×	×
Step 3 - Indentify unsafe control actions (UCA)	√	△	√	×	×	√
Step 4 - Identify loss scenarios	√	√	√	×	×	√
Step 5 - Propose solutions	×	×	×	√	√	√

Symbol definition √ : Suitable, △ : Suitable with modification, × : Not suitable

Ordinal measurement scale is the most commonly used scales in RPN. As defined previously, the range between ordinal measurement scale is not properly defined. The use multiplication process in the approach becomes questionable. For example, RPN of 8 can be obtained from (S,F,D) set of either (2,4,1) or (2,2,2). RPN calculation shows that both sets have equal importance. However, it is possible that the number 2 in the occurrence scale may have longer ranges while the number 4 in the occurrence scale may have shorter ranges. In this case, the possibility to get number 2 in the calculation, albeit with actual occurrence placed in the lower end of the ranges, becomes higher than to get number 4, with actual occurrence placed in the upper most of the range. The resulting RPN, after considering severity and detectability, may be equal. The RPN approach masks the relative importance between event that should have receive higher priority in the first case, which is (4,2,1). This weakness raises an alert on whether continue using the RPN approach is appropriate or not. Wheeler (2011), in his research, recommended to abandon the multiplication approach and use the information gained from the initial assessment to make the ranking instead.

4.3 Criteria for Prioritization in STPA

Basic STPA process is utilized as hazard analysis tool. Safety constraints produced by the analysis are used as requirements for system design. As discussed previously in section 3.6, the amount of produced safety constraints is large and needs to be prioritized. In order to prioritize them, modifications shall be made to the original process. After discussion about two safety philosophies in section 4.1, risk-based safety philosophy has been deemed capable to be used to prioritize the result of control-based safety philosophy. STPA itself adopts control based safety philosophy. Thus, an approach for risk-based decision making for STPA needs to be considered. RBDM term is selected in this case to emphasize that, in the proposed approach, risk is considered as the sole basis of decision making. However, stakeholders may add slight modification to the proposed approach to change it into RIDM if required.

The main focus of development approach is on how to integrate risk approach into the basic STPA process.

Three requirements have been defined to integrate RBDM approach into STPA. First, hazard and hazardous event shall be identified and analyzed by the approach. Second, an initial risk assessment shall be performed to determine the importance of each identified hazardous event and loss scenario. Third, the most optimum solutions shall be produced and delivered to the decision maker for final choice.

The first requirement have been covered by the process of STPA itself. STPA defines UCA as the hazardous event which leads into loss.

Some modifications are made for the second requirement. Risk assessment process can be performed together during the basic STPA process. It is because both UCA and causal scenario, which become the object of assessment, are the output of STPA.

For the third requirement, a problem is presented with the current approach. Basic STPA process stops after loss scenario is produced. No solution is provided and it is up to the stakeholder to determine what type of solutions are required to satisfy the safety constraints. Brainstorming approach is often used during this phase. Although they may seem to work perfectly, whether the selected solution is the most beneficial one or not is arguable. A systematic process should be added to determine the most optimum solution. In the proposed approach, additional step, step 5, shall be added after the final step of basic STPA.

STPA step 5 has an objective to propose solution for decision maker. Although no further research has been developed yet on how to determine the solution (it is still brainstorming), the added systematic process for solution recommendation assessment can be more convincing for the stakeholders. They may refer to the result of risk analysis to confirm whether the recommended solutions satisfies their initial requirement or not.

Relevant criteria that can be used for risk assessment and solution recommendation should be considered before proposing the detailed approach. During the initial risk assessment process, several relevant criteria have been identified. They are severity, likelihood, mitigation and level of knowledge. When solution is considered, a cost-benefit mindset is necessary. The relevant identified criteria for solution are cost, effectiveness and level of knowledge.

The following sections discuss thoroughly about each criterion and followed by evaluation to support the relevance claim. In each section, the criteria are assessed according to each step of STPA. The result of assessments have been summarized into Table 4.2. No relevant criteria has been identified in STPA step 2. It is due to the objective of the step which is to develop framework of system safety control structure and their interrelations. Neither Risk assessment nor solution assessment can be performed at this point since no information related to both assessment have been identified yet. For the other steps, at least two criteria can be included to perform prioritization.

4.3.1 Severity

Severity refers to the seriousness level of consequence, adverse effect, impact or loss that can happen to asset (Rausand, 2013, pg. 43). Typically, asset are classified into several categories which are human, environment and property, with human having the highest importance of the three. In some analysis, assets are given monetary value to make it easier to compare between each other. However, value of a human life is dubious and differs depend on analyst perception, causing the assignment of cost becomes more complicated. One example of severity classification can be seen in Table 4.3. The description provided under each conse-

Table 4.3: Severity Classes (Adapted from Rausand (2013, pg. 102))

Category	Consequence Type		
	People	Environment	Property
5. Catastrophic	Several fatalities	Irremediable damages to sea or seabed environment	Total loss of an equipment that results in long-term loss of production performance, where the cost of recovery is so significant that it totally eliminates the profit of field investment
4. Severe Loss	One fatality	Remediable damages, but with unacceptable long-term restitution time	Total loss of an equipment that results in long-term loss of production performance, where the cost of recovery reduces, but not totally eliminates, the profit of field investment
3. Major Damage	Permanent disability, prolonged hospital treatment	Remediable damages to sea or seabed environment with relatively short-term restitution time, however, where amount of damages is considered unacceptable by regulations or regulatory bodies	Total loss of an equipment that results in a short-term loss of production performance, where the cost of recovery reduces, but not totally eliminates, the profit of field investment
2. Damage	Medical treatment and lost-time injury	Remediable damages to sea or seabed environment with relatively short-term restitution time, where amount of damages is considered acceptable by regulations or regulatory bodies	Partial equipment damage which results in a short-term reduction of production performance
1. Minor Damage	Minor injury, annoyance, disturbance	Unnoticeable damages to sea or seabed environment	Unnoticeable impact on the production performance

quence type is used for assessment of loss qualitatively. Information about severity level of loss can be gathered from previous accident data from similar system. For each type of loss defined, worst-case severity level is commonly used for analysis to avoid multiple definitions of severity.

As discussed previously in section 2.3.1, STPA uses top down approach. It starts with definition of assets and losses that need to be avoided. During this phase, the severity level of each loss can be assessed directly. After definition of loss, STPA process continues with identification of system level hazard. System level hazard can be linked to the appropriate loss. The analysis process continues until UCAs and loss scenarios can be generated. It has been discussed before, that STPA results can be traced back to the top level due to their systematic refinement process. Therefore, by assigning severity level classification for each loss initially, the severity level can be inherited to each hazard, UCA and scenario.

Table 4.4: Likelihood Classes (Frequency)(Adapted from Rausand (2013, pg. 101))

Category	Frequency (/year)	Description
5. Fairly Normal	1 - 10	Event that is expected to occur frequently
4. Occasional	10^{-1} - 1	Event that happens now and then. The event will normally be experienced by the personnel
3. Possible	10^{-2} - 10^{-1}	Rare event, but will possibly be experienced by the personnel
2. Remote	10^{-3} - 10^{-2}	Very rare event that will not necessarily be experienced in any similar plant
1. Improbable	$< 10^{-3}$	Not foreseeable type of event

Table 4.5: Likelihood Classes (Probability) (Proposed Classification)

Category	Probability (%)	Description
3. High	20 - 100	High average of time / probability the system spend in this state
2. Medium	1 - 20	Medium average of time / probability the system spend in this state
1. Low	< 1	Low average of time / probability the system spend in this state

4.3.2 Likelihood

There are two definitions of likelihood that are used interchangeably for risk analysis. First, likelihood can denote the probability of occurrence of event(Rausand, 2013, pg. 33). Second, likelihood can also mean the frequency of an event happening in a certain period of time (Rausand, 2013, pg. 40). Both definitions can be used depending on the available data and the nature of thing to be assessed. For example, in the first definition, gathering relevant data to be used for likelihood assessment is very difficult. Most of the time the data is unavailable. In this case, bayesian approach, or sometimes called subjective probability, is often used. Analyst is required to assign numerical value from 0 to 1 that represent their belief to the likelihood of event. For the next definition, when relevant data is available, such as failure rate data, statistical distribution can be generated. This is called frequentist approach, where the frequency and/or probability can be obtained for the analysis. Example of classification for both type of likelihood can be seen in Table 4.4 and 4.5.

In STPA, the likelihood can only be determined after the event, in this case UCA, have been identified. Thus, likelihood assessment can only be performed starting from STPA step 3. However, UCA consist of combination between two conditions, control action and conditional event. Both conditions need to be achieved simultaneously in order to become a UCA. When assessing conditional event, both frequentist and bayesian approach can be used. However, for the control action, the likelihood is more difficult to assess. The reason is because the control action is conditional to the causal factor that influence the controller. During this step, the causal factor has not been identified yet. It can only be performed after STPA step 4 where loss scenario and causal factor have been identified. Therefore, the likelihood assessment of UCA in step 3 can only serve as indirect assessment from likelihood of conditional event. If the differences between conditional events are significance, then the assessment should be performed here. If the differences is insignificant, then likeli-

Table 4.6: Mitigation Possibility Classes (Proposed Classification)

Category	Description
5. Impossible	The process safety time is so short that it is impossible to interact and as such avoid the consequences of the UCA
4. Unlikely	The process safety time is moderate, but there is low possibility to allow an interaction that avoids the consequence of the UCA
3. Possible	The process safety time is moderate, but there is moderate possibility to allow an interaction that avoids the consequence of the UCA
2. Likely	The process safety time is moderate, but there is high possibility to allow an interaction that avoids the consequences of the UCA
1. Certain	The process safety time is sufficient to allow an interaction that avoids the consequences of the UCA

hood assessment should better be performed after STPA step 4 where both causal factor and conditional event information can be gathered.

4.3.3 Mitigation Possibility

Mitigation possibility is a modification from detectability criteria that is originally used for RPN ranking in FMECA. Mitigation possibility is defined as an assessment of the probability to prevent / mitigate the unwanted event before resulting into a loss. Mitigation possibility assessment requires information about detection time, response time and event escalation time to loss. An example of mitigation possibility classification can be seen in Table 4.6. It should be noted that subjective judgement, or bayesian approach, will be mostly used for the assessment. For example, a hazardous event of uncontrolled steering wheel when driving on the highway is selected. In this case, the detection time of event is short due to the driver awareness of the driving situation. However, the response time can be fast or slow depending on the driver experience, cause of uncontrolled steering wheel, etc. Additionally, the time required from being unable to control the steering wheel to result into an accident is quite fast. By combining these information and using worst-case approach for the response time assumption, the assessment of mitigation possibility concluded as unlikely. It should be noted that the background information related to these assumptions are required to be noted to indicate the basis for analysis.

Mitigation possibility criteria is closely related to the hazardous event. In STPA, UCA is the hazardous event. Thus, mitigation possibility assessment can be performed after step 3 analysis where UCAs have been identified. Mitigation possibility criteria is one of the criteria used for risk assessment. The top down approach of STPA can be used to inherit the information of mitigation possibility assessment from UCA to each loss scenario. Despite the differences of causal factors and scenario that cause each UCA, the mitigation possibility assessment stays the same (only based on the value during UCA assessment). This is due to the viewpoint for judging the mitigation possibility based on the effect of UCA. Thus, the different required time that each causal factor may have before causing a UCA is neglected during the assessment.

Table 4.7: Cost Classes (Proposed Classification)

Category	Comparison to Allocated Budget	Description		
		CAPEX	OPEX	Total Cost
5. Almost None	< 0.2	Minimum relative cost for initial investment	Minimum relative cost for operational cost	Minimum relative cost for CAPEX & OPEX
4. Economical	0.2 - 0.8	Low relative cost for initial investment	Low relative cost for operational cost	Low relative cost for CAPEX & OPEX
3. Moderate	0.8 - 1.2	Moderate relative cost for initial investment	Moderate relative cost for operational cost	Moderate relative cost for CAPEX & OPEX
2. Expensive	1.2 - 2	High relative cost for initial investment	High relative cost for operational cost	High relative cost for CAPEX & OPEX
1. Very Expensive	> 2	Very high relative cost for initial investment	Very high relative cost for operational cost	Very high relative cost for CAPEX & OPEX

4.3.4 Cost

Additional cost will incur when proposing solution for a problem. The cost is associated with either capital expenditure (CAPEX) or operational expenditure (OPEX). CAPEX covers the cost of purchase, installation, resource and training. OPEX covers the cost of operation and maintenance. Frequently, the proposed solutions are more than one. Although it is important to reduce the problem, the cost should not exceed the allocated budget. Thus, assessing which solution has the least cost while providing maximum benefit is important. The cost criteria is split into CAPEX and OPEX. The reason is because project at different stage may have different priority. During initial project stage, major changes can still be made because the complete system has not been established yet. Preventive measures can still be made. Thus, making assessment of CAPEX becomes more important than OPEX. Next is during commissioning stage. When some of the system have been decided, the flexibility of changes becomes minimal. Therefore, only reactive measures can be made based on the current system. To ensure that the solution does not become too expensive, assessment of OPEX becomes more important than CAPEX. Depending on the requirement, either CAPEX, OPEX or both CAPEX & OPEX can be included for cost assessment. An example for cost classification can be seen in Table 4.7.

The cost of proposed solution can be assessed only when solution for the problem has been identified. Thus, cost criterion is relevant only after STPA step 5.

Table 4.8: Effectiveness Classes (Proposed Classification)

Category	Description
5. Effective	No residual risk. Applicable for most software related error solution
4. Major effect	Minimum residual risk.
3. Moderate Effect	Moderate residual risk. May need another solution
2. Slight Effect	High residual risk. Several more solutions are necessary
1. Ineffective	Similar residual risk. The effect cannot be seen. Other solutions are preferable

4.3.5 Effectiveness

Effectiveness refers to the benefit effect of proposed solution in reducing risk (Rausand, 2013, pg.112). As mentioned earlier in section 4.3.4, effectiveness criteria is inseparable with the cost criteria. For example, when proposing solution to reduce the possibility of human error, there can be two solutions. The solutions are either to provide training to human or to automate the system. It can be estimated clearly that automation is more reliable option than training. However, the cost incurred is way more expensive than the other option. This type of dilemma is common when proposing a solution. Therefore, it is up to the company policy to decide the acceptance criteria. Example of effectiveness classification can be seen in Table 4.8.

Similar to cost criterion, effectiveness assessment can be performed only after the solution has been proposed. Thus, effectiveness criterion can be assessed only after STPA step 5 .

4.3.6 Level of Knowledge

Level of knowledge, or knowledge for short, has capability to depict the uncertainty factor hidden from the assessment. Assessment is always dependent to the knowledge of information gathered. If the information is changed, analyst is ideally required to update the result of the analysis. However, this is often not the case. The results are often taken for granted and the stakeholder becomes confident with the assessment result without confirming whether the current condition still satisfy the initial conditional assumption. This is one of the reason why Leveson (2011), when developing STAMP/STPA, has skepticism to the use of risk-based approach for assessing the safety of a system. For example, systematic error, such as design factor, cannot be easily quantified into neither probability nor frequency. Thus, systematic error is either neglected or still used by assigning number without scientific explanation. For the latter case, bayesian approach is often used. The resulting assessment differs depending on the nature of the analyst (either optimist, neutral or pessimist). If the numbers produced by the assessment can be heterogeneous, then the validity of the result becomes questionable. However, quantification of risk is still necessary in order to understand the differences of importance between one event to another. Thus, Flage and Aven (2009) recommended that each risk assessment is required to include the background knowledge used for assumption. Then, the information can be treated separately based on the systematic treatment proposed by Berner and Flage (2016). Example of level of knowledge classification can be seen in Table 4.9.

In risk-based safety philosophy, level of knowledge is a supporting criteria for other criteria such as severity, likelihood, mitigation, cost and effectiveness. In STPA, the level of

Table 4.9: Level of Knowledge Classes (Adapted from Flage and Aven (2009))

Category	Description
5. Weak	* The phenomena involved are unknown. No similar phenomena have been observed previously * The models are non-existent or known/believed to give poor predictions * Unreasonable assumptions made which represent strong simplifications. * Data are not available, or are unreliable. * There is lack of agreement/consensus among experts.
3. Moderate	* The phenomena involved are unusual. Similar phenomena may be used as reference * The models used are considered simple/crude * The assumptions made are reasonable, however, there are many simplifications * Some reliable data are available.
1. Strong	* The phenomena involved are common. Well understanding to of the phenomena * The models used are known to give predictions with required accuracy * The assumptions made are seen as very reasonable. Few simplifications are made * Most of reliable data are available. * There is broad agreement among experts

knowledge can be used when assessing severity, to determine whether there is sufficient understanding about loss phenomena. If it is insufficient, the analyst is required to gather more information about the phenomena before proceeding to the next analysis. Afterwards, during the assessment of both mitigation and likelihood, the decision maker is required to be informed regarding the uncertainty of both assessments. Level of knowledge is also applicable at this step. When assessing the solutions, reference information about cost and effectiveness of solutions are dependent to the assumption of condition where they are going to be implemented. The assumptions should be recorded as background knowledge level. For conclusion, level of knowledge criteria can be used after step 1, step 3, step 4 and step 5 of STPA.

4.4 Prioritization Approach for STPA (PA-STPA)

Prioritization approach for STPA (PA-STPA) is proposed as the name of RBDM approach with STPA. The general objective of PA-STPA is to produce the most optimum solutions in order to achieve system safety. Specifically, there are three objectives that answer the requirements discussed in previous section 4.3. The refined objectives are identify and analyze hazard, assess the hazard risk, and produce the most optimum solution. The approach adopts semi-quantitative risk analysis approach and use relevant criteria for assessment. Relevant criteria are previously discussed in section 4.3. An illustration of how the proposed approach differs from the basic STPA can be seen in Figure 4.2.

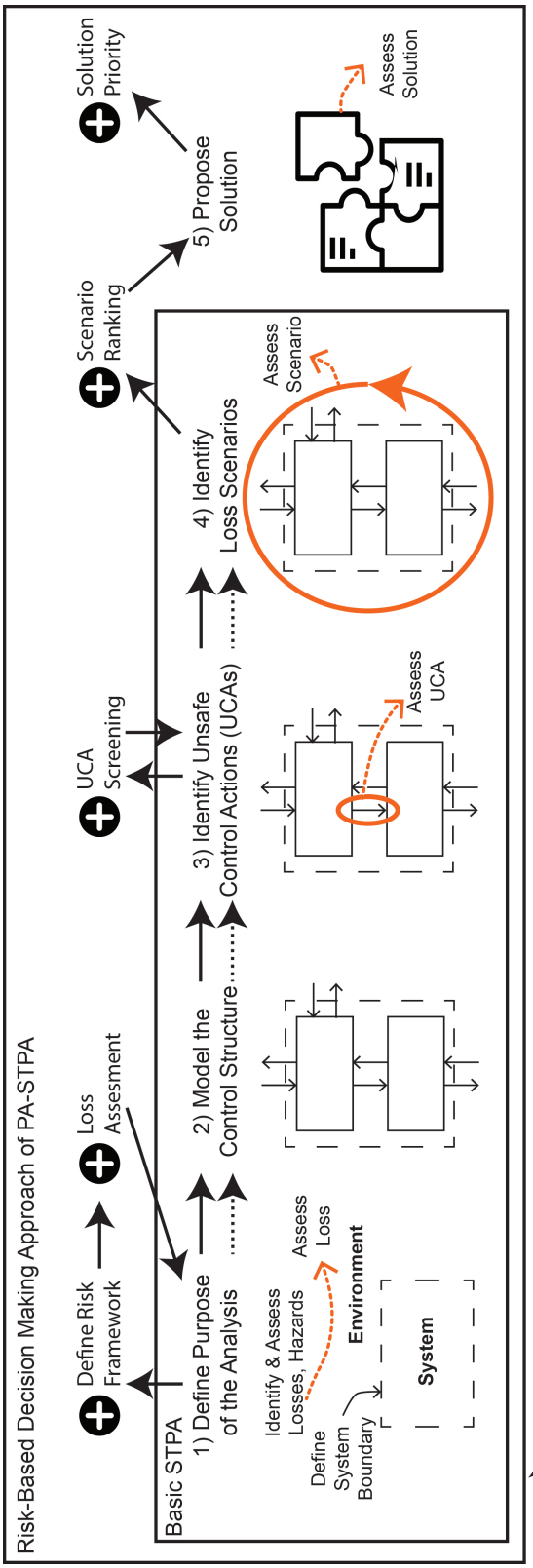


Figure 4.2: PA-STPA Processes

PA-STPA consists of 5 steps, 4 of which come from the basic STPA. Additional main step is added at the end to propose solution for stakeholders. In-between some of the main step and after the final step, additional processes are added to perform the risk prioritization approach. There are four in-between steps and one final step which are define risk framework, loss assessment, UCA screening, scenario ranking and solution priority.

In the step of risk prioritization approach, criteria that have been discussed before are integrated to PA-STPA based on Table 4.2. The severity, likelihood (frequency), mitigation possibility, cost and effectiveness criteria are classified into five levels. The classification can be seen from Table 4.3, 4.4, 4.6, 4.7 and 4.8. The reason of using five level classification is to increase the sensitivity of assessment. Likelihood (probability) and level of knowledge are classified into only three levels (see Figure 4.5 and 4.9). For the likelihood (probability), it is used in STPA step 3 for UCA screening. During this process, only limited information available. The criterion is used only for an indirect assessment. The importance of having more sensitive classification is minimal. For level of knowledge, the differences between each classification are vague. As seen in Table 4.9, the description of each category is pure qualitative judgment. It cannot be compared with the other criteria such as likelihood where range of value can be obtained through further analysis. Adding more classification level between the current category will reduce the accuracy of assessment and increase confusion for the analyst. For the part where level of knowledge is used in the calculation, the class assigned numbers are adjusted into 1,3 and 5. This adjustment ensures that the importance of the criterion becomes equal to other criteria.

The following section explained the proposed detailed process for the new added steps.

4.4.1 Loss Assessment in STPA Step 1

During PA-STPA step 1, two additional tasks are added. The tasks are to define risk framework for the following analysis and to perform loss assessment. Updated detailed flowchart for PA-STPA step 1 can be seen in Figure 4.3. The first task objective is to establish acceptance criteria for risk assessment and solution recommendation. For the latter task, the relevance of identified loss is assessed. The loss assessment is used to determine whether the loss phenomena is relevant for the following analysis. Two criteria used for assessment are severity and level of knowledge. After the process of PA-STPA step 1 has been concluded, it continues to the basic STPA step 2 explained previously in section 2.3.

Step 1.1 (Updated) Plan and prepare

In addition with the previously defined process during this step, the analyst is required to define the approach for the whole risk assessment process. There are four approaches that should be established: loss assessment approach, UCA screening approach, scenario ranking approach and solution priority approach. The defined approaches are used to determine how the assessment process is going to be performed in each PA-STPA step. The available options for each assessment are presented later during explanation for each step.

Step 1.4 (New) Assess severity, record assumptions and measure level of knowledge

In this step, three activities should be performed. They are severity assessment, record the assumptions pertaining to the loss and measure the level of knowledge. The severity is assessed based on relevant experience data and expert judgments about loss. The level of knowledge indicates the uncertainty about the knowledge information of loss severity based on the recorded assumptions. The classification of severity and level of knowledge refer to

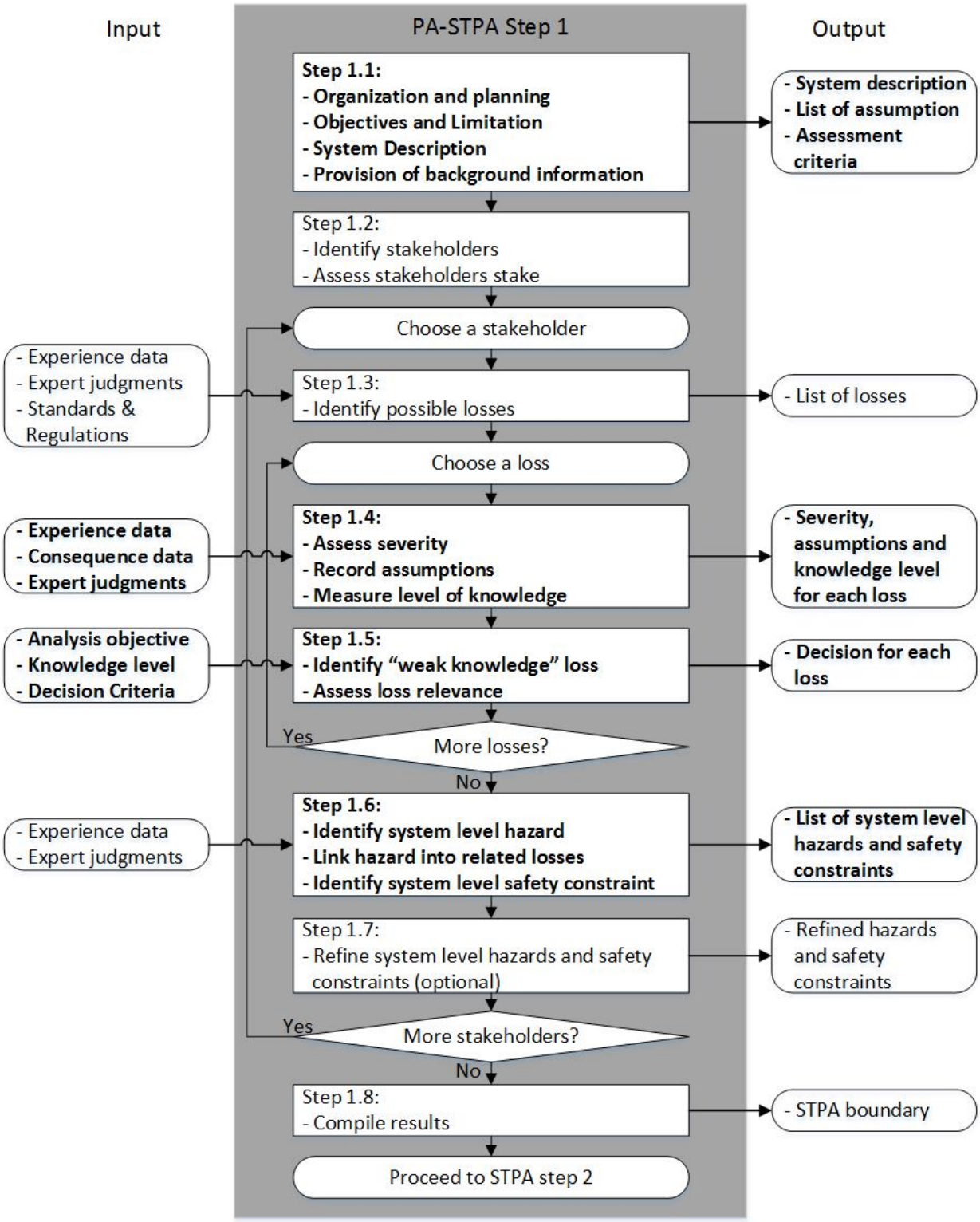


Figure 4.3: PA-STPA Step 1 Flowchart

the proposed classification on Table 4.3 and Table 4.9.

Step 1.5 (New) Identify "weak knowledge" loss & assess loss relevance

There are two processes in this step: identification of weak knowledge loss and relevance assessment of the loss.

First, identification of weak knowledge loss is performed by checking the level of knowledge associated with a loss. If the knowledge about loss phenomena is low, the analysis should be stopped and another side step should be performed. The analyst is then required to identify what kind of additional information can be gathered to reduce the uncertainty. If gathering additional knowledge is impossible, then the loss should be given higher caution priority and informed to the decision maker.

Second, the relevance of loss is checked based on the acceptance criteria. There are two parameters that can be used: minimum severity level or use qualitative judgment according to the analysis purpose. For example, if one of the identified loss does not meet the minimum acceptable severity level, it can still be included in the analysis if the analysis objective specifically required to identify the risk related to that loss. If no requirement has been made, then the loss that does not meet the minimum criteria should be screened out.

Step 1.6 (Updated) Identify system level hazards and safety constraints

After identification of system level hazards, the severity of each loss is linked to the hazards. If the hazard has a possibility to lead into several losses, the worst-case approach is used. Highest severity level is then assigned to the hazard.

4.4.2 UCA Screening in STPA Step 3

After UCA has been identified, prioritization can be performed. The process is called UCA screening. The objective is to reduce the amount of "low priority" UCA in the following analysis. The criteria for screening are severity, conditional event likelihood, mitigation possibility and level of knowledge. Detailed flowchart of the process can refer to Figure 4.4.

Step 3.3 (New) Inherit severity, estimate conditional event likelihood, assess mitigation possibility, record assumptions and measure level of knowledge

During this step, five activities need to be performed. First, the severity level of UCA should be inherited from the severity of the linked hazard using the worst-case approach. Next, the analyst is required to estimate likelihood of the conditional event. Afterwards, mitigation possibility of UCA should be assessed. Finally, information from likelihood and mitigation possibility assessment shall be recorded for uncertainty factor and then measured for UCA level of knowledge. The classification of likelihood, mitigation and level of knowledge each refers to the proposed classification from Table 4.5, 4.6 and 4.9 in sequence.

As discussed previously in section 4.3.2, UCA is combination of both conditional event and control actions. Due to minimal information about the likelihood of control action, which is influenced by the causal factor, the likelihood of UCA cannot be estimated yet. Thus, the current likelihood assessment can only serve as an indirect measure for the possible likelihood of UCA. However, it should be noted that the likelihood value of conditional event becomes the limiting constraint of the likelihood value of scenario that will be obtained later. When multiplying probability and frequency values, if the probability value is very low, then the multiplication result will be lower by several degree. Thus, it can lower the risk of UCA considerably

Step 3.4 (New) Calculate UCAPN and filter UCA

In this stage, priority for each UCA is calculated and assessed according to the UCA screening criteria. The UCA priority number (UCAPN) is calculated by using the formula

$$UCAPN = S \times M \times K \tag{4.1}$$

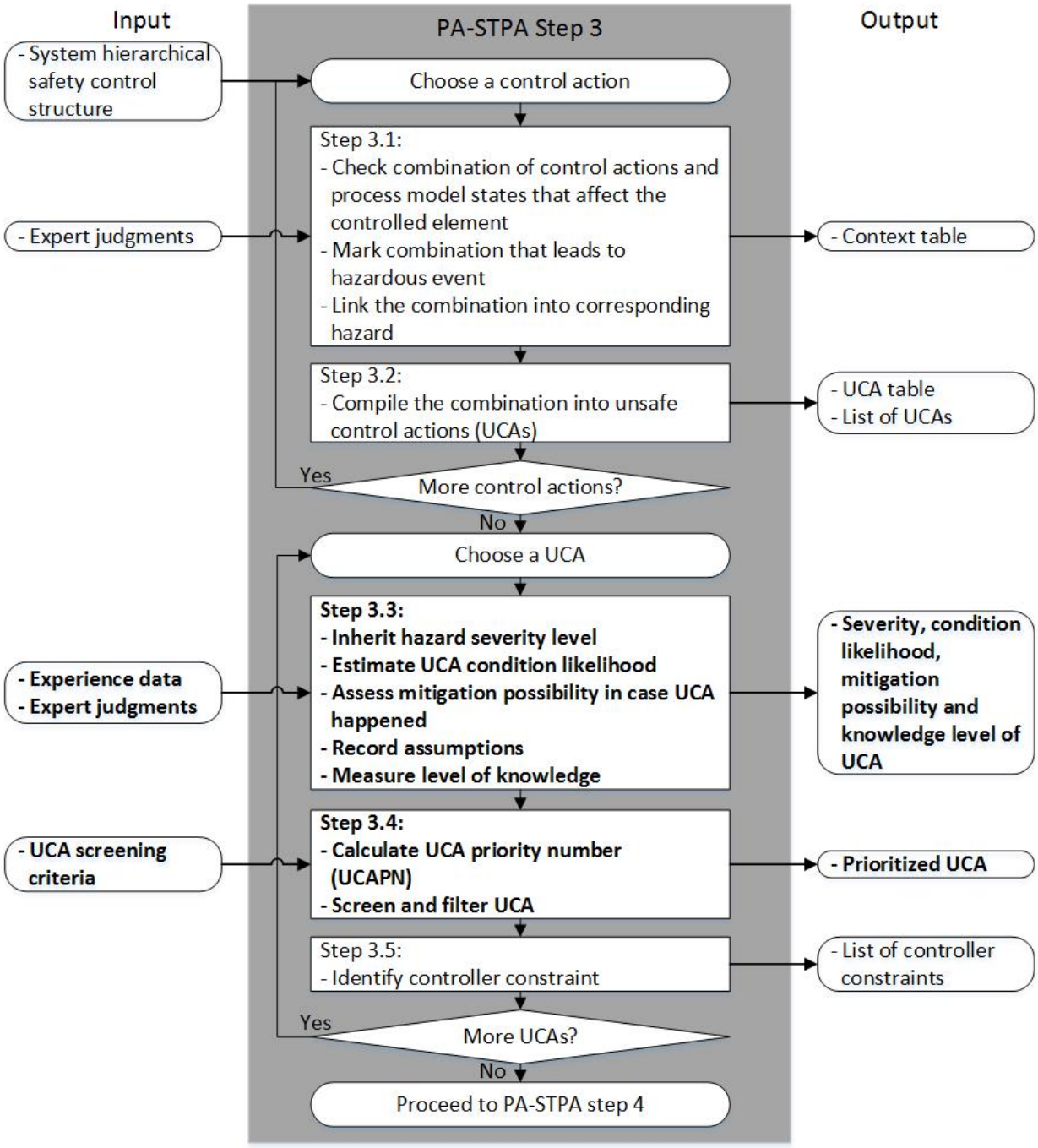


Figure 4.4: PA-STPA Step 3 Flowchart

Table 4.10: UCA Priority Assessment Category

UCAPN	Assessment
40 - 125	High priority
10 - 39	Medium priority
1 - 9	Low priority

With S = Severity; M= Mitigation; K = Level of Knowledge

The formula is a modification from the original risk formula, $R = S \times L$. During this stage, the likelihood is only an indirect measure. Therefore, it should not be included in the formula yet. Mitigation is added to the calculation since the criterion indicates the possibility of UCA causing loss(es). Although the calculation result becomes beyond the original notion of risk, the author still considered it as reasonable to be included due to some logical reasoning. For example, consider a case of two UCAs with similar severity level but has different mitigation possibility level. For the one with lower mitigation possibility level, the prevention possibility is higher. Therefore, the risk of this UCA is arguably lower than the other UCA with higher mitigation possibility level. As mentioned previously, Level of knowledge indicates the uncertainty of other criteria. Thus the risk value becomes uncertain and needs to be calibrated by including the uncertainty factor into the multiplication formula. Level of knowledge only has 3 classification level. The influence of the criteria should be adjusted by changing the value of each criteria into an increment of 2, instead of 1 (e.g 1,3,5. see Table 4.9).

The UCAPN can be classified into three category of high, medium and low priority, as seen in Table 4.10. The range is obtained from the modification of original risk matrix range in Table 4.1 with two criteria into the current range of UCAPN which has three criteria. Distribution of combinations within each range is tried to be maintained as similar as possible to the original range.

There are two approaches that can be used to filter UCA. First, using only the minimum acceptance criteria of UCAPN as the parameter. Second, including conditional event likelihood as an additional parameter, instead of just UCAPN. The second approach is only applicable when the differences between conditional event likelihood is significant. For example, when there are UCA with high/medium probability of conditional event compared to UCA with low probability of conditional event. In this case, the risk of the first UCA will be mostly higher than the second UCA due to the reason mentioned in the final paragraph of previous step 3.3. Thus, the minimum UCAPN acceptance criteria for UCA with low probability of conditional event can be increased since the risk of those UCA shall be lower. However, if the differences between conditional event likelihood is insignificant, the first approach should be used. The first approach is more conservative than the second approach as it screened out lower number of UCA than the latter. UCA that does not satisfy the screening criteria is screened out and not included to the following analysis.

4.4.3 Scenario Ranking in STPA Step 4

After loss scenarios has been identified, scenario can be prioritized. The objective is to determine scenarios with higher priority and ranked them in order. The criteria for ranking are severity, likelihood, mitigation and level of knowledge. Figure 4.5 represents the updated detailed flowchart of the process.

Step 4.2 (New) Identify scenario causal factors (CF)

Based on the loss scenario, causal factors (CF) can be determined. The causal factors should not be limited by only failure-based factor. It can also be due to interaction problem such as miscommunication or duplicate control action.

Step 4.3 (New) Inherit severity, conditional event likelihood, mitigation possibility, and UCA level of knowledge, estimate scenario likelihood, record assumptions and measure combined level of knowledge

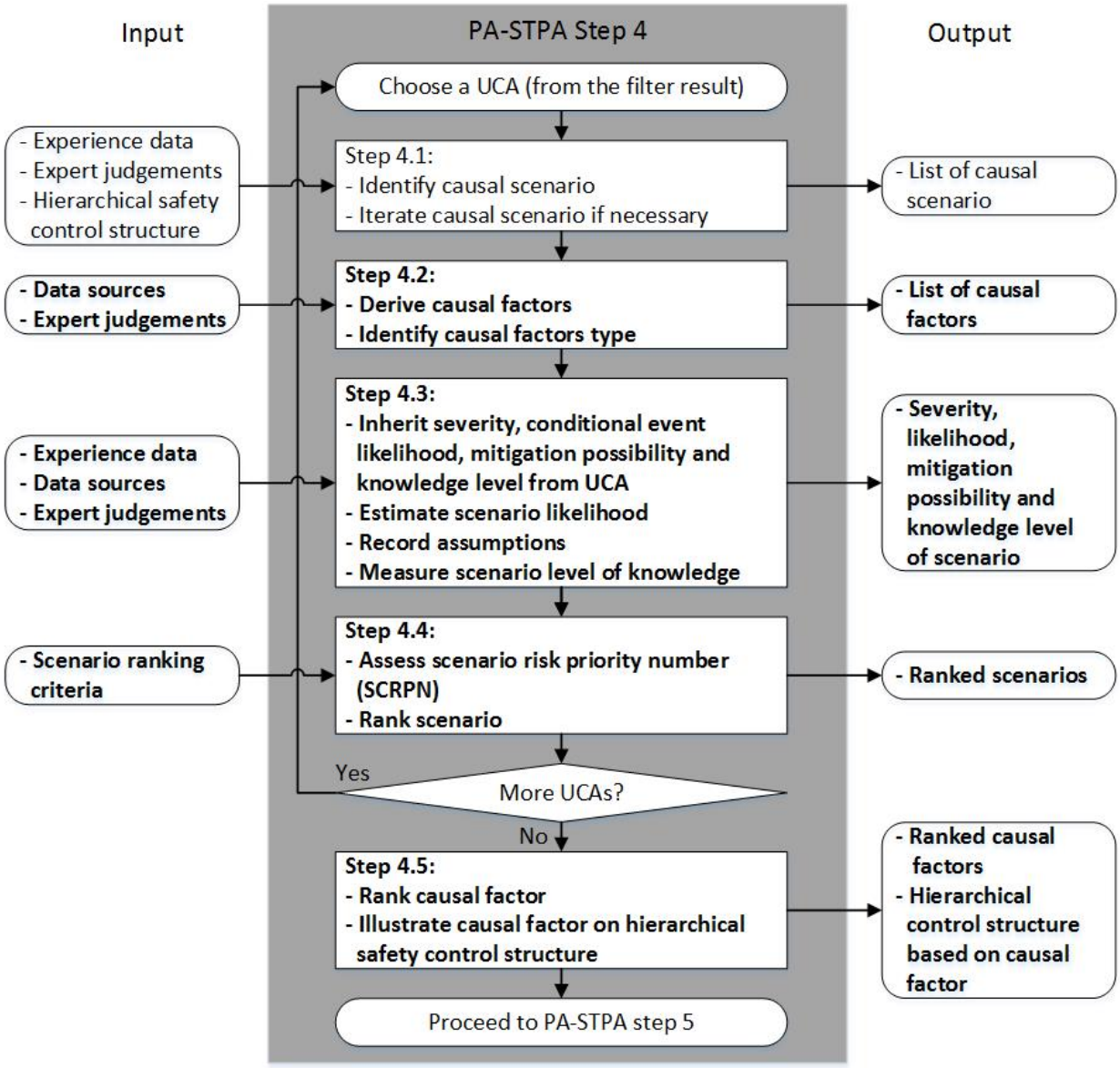


Figure 4.5: PA-STPA Step 4 Flowchart

In this phase, four activities are required to perform. First the value of severity, conditional event likelihood, mitigation possibility and UCA level of knowledge are inherited from linked UCA to each loss scenario. Afterwards, the analyst is required to estimate the scenario likelihood and combined it with conditional event likelihood. The assumptions for scenario likelihood is recorded and then measured for the combined level of knowledge. The classification of scenario likelihood and level of knowledge are based on the proposed classification from Table 4.4 and 4.9. Specific to background knowledge assessment, there are two different knowledge assessment information from UCA and CF. The information needs to be combined together into the knowledge level of scenario. The assessment with higher uncertainty, or having weaker knowledge, is assigned for the scenario level of knowledge.

Step 4.4 (New) Assess SCRPN and rank scenario

The risk of each loss scenarios is calculated to obtain the risk picture. The scenario risk

Table 4.11: Scenario Risk Assessment Category

SCRPN	Assessment
100 - 625	Unacceptable
26 - 99	ALARP
1 - 25	Broadly acceptable

priority number (SCRPN), is calculated by using the formula

$$SCRPN = S \times M \times L \times K \tag{4.2}$$

with S= Severity; M = Mitigation; L = Likelihood; K = Level of Knowledge

Similar to the formula UCAPN from step 3.4, the current formula is a modification from the original risk formula. However, in the current stage, the likelihood assessment has been obtained. Therefore, it is included now for risk calculation. The level of knowledge class assigned numbers are similarly adjusted for the calculation since it is the only criterion with three level of classification.

The SCRPN can be classified into three category of broadly acceptable, ALARP and unacceptable risk, as seen in Table 4.11. The range is obtained through similar approach to obtain the range in Table 4.10. It is obtained by modifying the original risk matrix range for each category. The SCRPN range is adjusted for four criteria with similar distribution of combinations within each range.

The produced scenario risk should be mostly distributed on either high or ALARP risk. It is because low priority UCA has been screened out already, reducing the possibility of having low-risk scenario. The scenarios are then ranked from high to low to denote which scenario has higher priority than the other.

Step 4.5 (New) Rank causal factor and produce CF hierarchical safety control structure

The scenarios can be classified into several causal factors. The causal factors are summarized and listed in the order of priority. The ranking is based on the value of SCRPN. If the causal factor has multiple SCRPN values, only the highest value is considered. The causal factors are then added to the original hierarchical safety control structure as an information for the decision maker.

Screening of causal factors can be performed at this point. Causal factor with acceptable risk can be screened out from the analysis.

4.4.4 Solution Priority in STPA Step 5

The new step is added in order to integrate the final step prior to decision making into STPA. In this stage solution is proposed based on the causal factor. Afterwards, the solution can be prioritized. The objective is to determine the most optimum solution for system safety. The criteria for ranking are cost and effectiveness. Figure 4.6 illustrates the updated detailed flowchart of the process.

Step 5.1 (New) Propose solution

Based on each causal factors, different solutions can be proposed. Solution is proposed through the brainstorming approach. If multiple solutions are available, prioritization should be performed

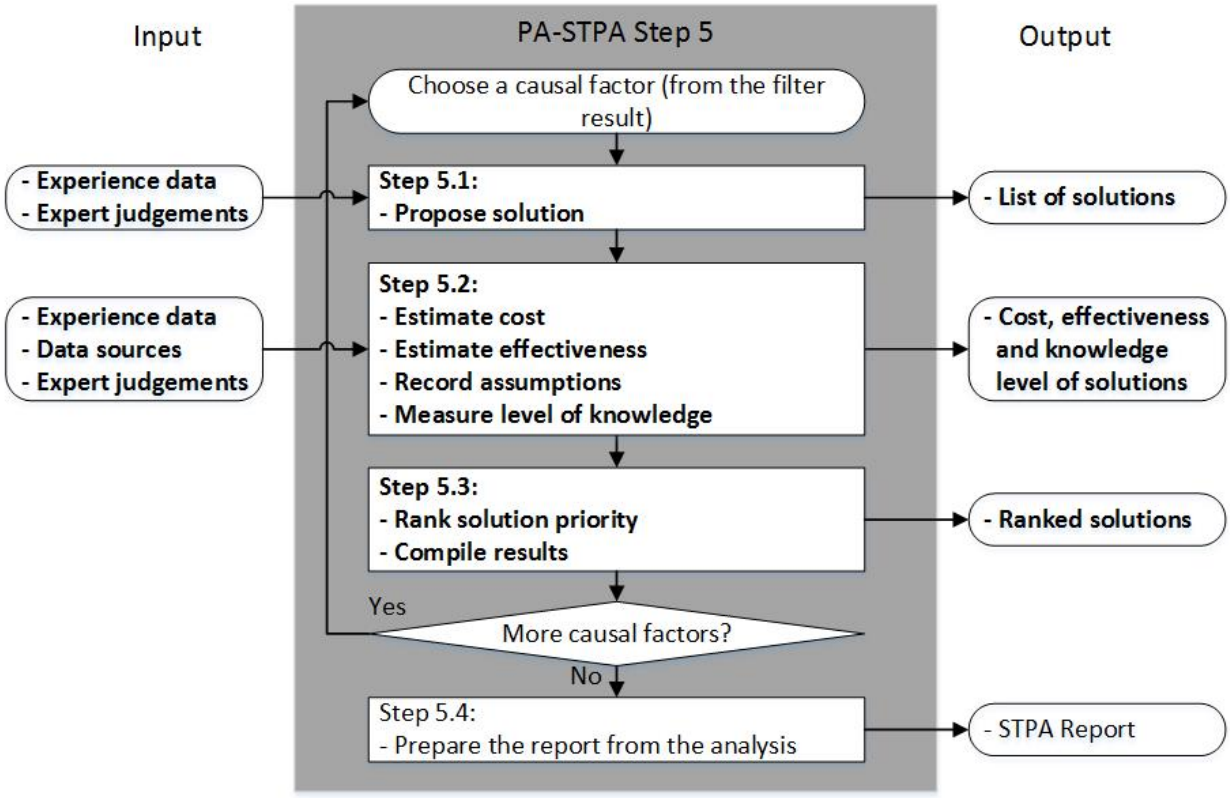


Figure 4.6: PA-STPA Step 5 Flowchart

Step 5.2 (New) Estimate cost and effectiveness, record assumptions and measure solution level of knowledge

During this step, four activities should be performed. First, the analyst needs to estimate cost which consists of CAPEX and OPEX based on the current market value of the solutions. Afterwards effectiveness of each solution should be estimated. The assumptions for each criterion are recorded and then measured into the level of knowledge of solution. The classification of cost, effectiveness and level of knowledge are based on the proposed classification from Table 4.7, Table 4.8 and Table 4.9.

Step 5.3 (New) Calculate SOLPN and rank solution

The priority of each solution is calculated and ranked in the order of priority. The solution priority number (SOLPN) is calculated by using the formula

$$SOLPN = C \times E \times K \tag{4.3}$$

with C = Cost (CAPEX/OPEX/Both), E = Effectiveness, K = Level of knowledge

The formula is obtained by multiplication of the three criteria. It is based on logical reasoning that by increasing the effectiveness and cost at the same time, the priority of solution should be increased as well. The reasoning is also applied otherwise. Depending on the requirement, the cost assessment can include either only CAPEX, OPEX or both. Level of knowledge is used for the uncertainty within each priority number. The classification number of level of knowledge is adjusted to 1,3 and 5 to equalize the importance of the criterion.

Chapter 5

PA-STPA Implementation for Subsea Gate Box

The objective of this chapter is to present the result of using PA-STPA to identify and analyze the hazard of the subsea gate box. The presented results are only those that differs from the basic STPA result presented earlier in Chapter 3. The chapter begins by defining the assessment approach for the PA-STPA analysis of SGB system. Afterwards, loss, UCA, scenario and solutions were assessed according to the proposed approach explained in Section 4.4. Finally, brief discussions of the results are presented at the end of each section.

5.1 Assessment Approach

Four approaches had been defined as framework for risk-based decision making approach in PA-STPA: loss assessment approach, UCA screening approach, scenario ranking approach and solution priority approach. The approaches were tailored for analysis of subsea gate box system that was currently in early system development phase. The approaches specified how loss assessment, UCA screening, scenario ranking and solution priority are going to be performed.

Loss assessment approach

First was the loss assessment process approach. There were two criteria for assessment: severity and level of knowledge. The assessment approach was semi-quantitative based on qualitative judgment.

Loss that had weak level of knowledge required additional process. The analyst was required to gather more information, either by performing simulation or obtaining historical data related to the loss. If it was impossible to reduce the uncertainty, the results should be recorded and informed to the decision maker.

The relevance of loss was then assessed. It was classified into two types: "included" and "screened out". "Included" was given for loss that should be analyzed further. "Screened out" was given for loss that should be left out from further consideration.

There were two parameters used for the assessment: analysis objective and severity. The relevance assessment process was elaborated for explanation. First, the objective of the analysis was checked. If the analysis objective was aligned with the identified loss, then the loss was "included". If otherwise, then the severity of the loss was checked. Minimum severity level was assigned as screening parameter. For example in SGB, if the severity of the loss was considered as major damage or more severe ($S \geq 3$), then the loss was "included" for the

Table 5.1: Loss Relevance Assessment Criteria

Assessment	Parameter
Included	* Identified loss is the objective of the analysis (First priority, if clashed with other condition, refer to this criteria) * Severity ≥ 3
Screened Out	* Identified loss is not the objective of the analysis (First priority, if clashed with other condition, refer to this criteria) * Severity < 3

Table 5.2: UCA Screening Criteria

Assessment	Parameter
Included	* Conditional event likelihood = high/medium and UCAPN ≥ 10 (high and medium priority) * Conditional event likelihood = low and UCAPN ≥ 25 (high and upper half of medium priority)
Screened Out	* Conditional event likelihood = high/medium and UCAPN < 10 (low priority) * Conditional event likelihood = low and UCAPN < 25 (low and lower half of medium priority)

analysis. The loss that did not conform with both conditions should be "screened out" from the analysis. The loss relevance acceptance criteria is summarized into Table 5.1.

UCA screening approach

Second was the UCA screening approach. There were four criteria used for assessment: severity, conditional event likelihood, mitigation possibility and level of knowledge. Severity was inherited from the loss assessment result. The assessment approaches for the three other criteria were semi-quantitative approach based on qualitative judgment.

The second approach specified in section 4.4.2 step 3.4 was used for acceptance criteria. Two parameters were used for the acceptance criteria: conditional event likelihood and UCAPN value. These were due to the different operational modes of SGB that are investigated in the analysis. Set point adjustment operation was assumed to occupy, in average, more operational time than bypass operation. The differences were considered significant. Differentiation between the acceptance value of UCAPN between both operations type was judged as reasonable.

UCAs were classified according to their priority from set range in Table 4.10. High and medium likelihood of conditional event had minimum passing line of UCAPN ≥ 10. It meant that all medium and high priority UCAs were included. UCAs with lower UCAPN value should be screened out from the assessment. In another case, for low likelihood of conditional event, the minimum passing line was slightly higher, with UCAPN ≥ 15. It meant that most medium priority and all high priority UCAs were included. The UCA screening acceptance criteria is summarized into Table 5.2.

Scenario ranking approach

Third was the scenario ranking approach. There were four criteria used for assessment: severity, likelihood, mitigation possibility and level of knowledge. Severity, conditional event

likelihood mitigation possibility and UCA level of knowledge are inherited from the UCA assessment results. The assessment approaches for the scenario likelihood and knowledge level criteria were different.

Scenario likelihood consists of conditional event likelihood and causal factor likelihood. Quantitative data were available for some of the causal factors. Two approaches were used based on the type of causal factor. If the causal factor was hardware failure, information from Oreda (2002) was mostly used to obtain the likelihood. Otherwise, if either human or systematic error was the cause, bayesian approach should be used for estimation. Therefore, likelihood used semi-quantitative approach based on either quantitative or qualitative judgment. For level of knowledge, only qualitative judgment is used for the semi-quantitative approach.

Scenarios were ranked in order from high to low based on the value of SCRPN to determine the priority. The risk of resulting scenario would be distributed mostly in either ALARP or unacceptable region due to UCA screening. Additional screening was therefore deemed unnecessary. The causal factor ranking gained during this process was also ranked from higher to lower value of SCRPN, with high number denotes higher risk.

Solution priority approach

Last was solution priority approach. Prioritization was performed for the recommended solutions. There were three criteria used for assessment: cost, efficiency and level of knowledge. Semi-quantitative approach based on qualitative judgment was used for all three criteria. For cost criteria, both CAPEX and OPEX were considered together. The solution with higher SOLPN for each causal factor was then proposed to decision maker for final choice.

5.2 Loss Assessment & Update System Level Hazard

Three losses were identified: environment pollution, costly equipment damage, unnecessary loss of production. Each loss was judged against two criteria: severity and knowledge. Loss relevance assessment was performed to determine whether the identified loss should be included or not.

This section is separated into three subsections: assessment process, loss relevance assessment and discussion and loss assessment result. Assessment process elaborates the procedure to obtain the classification level for both criteria. Loss relevance assessment determine the relevance of identified loss for following analysis. Loss assessment result presents the additional results obtained during PA-STPA step 1.

Assessment Process

An example of assessment process is provided for environmental pollution. The loss was assessed against two criteria: severity and level of knowledge.

This loss was judged to have severity level as severe loss (4). This was due to the difficulty to clean oil spill from the sea if leakage happened. Deepwater horizon was one of the major accident which resulted into oil spill (BP, 2010). It required several years for the oil to be cleaned into acceptable level.

Environmental pollution happened quite often for both subsea and offshore installations. The information that was used as reference was considered reasonable with some simplifications. The level of knowledge was judged as moderate (3).

Table 5.3: Loss Relevance Assessment Results (Example)

No	Loss	Severity	Knowledge	Assumption	Assessment	Supporting Reason
1	Environmental pollution	4	3	* Worst-case consequences * Limited information on relevant accident data (mostly are hydrocarbon spills offshore)	Included	* Possible to happen in all subsea system * Often happen topside
2	Costly equipment damage	3	3	* Worst-case consequences * Production is available through other process line (bypass or other SGB) * High cost of equipment recovery	Included	* Difficulty to access the equipment * Equipment failure is sometime unpredictable / limited degradation model * Expensive inspection, maintenance and repair (IMR)
3	Unnecessary loss of production	2	3	* Worst-case consequences * Short term loss of production performance * Production is available through other process line (bypass or other SGB)	Included	* Difficulty to access the equipment * Equipment failure is sometime unpredictable / limited degradation model * Production availability and efficiency is the main function of SGB

Similar assessment processes were performed to all three losses. Assumptions used for assessment were recorded for reference. They are summarized into Table 5.3.

Loss relevance assessment and discussion

Table 5.3 presents the summary of loss relevance assessment results. According to the loss relevance acceptance criteria, all three losses were assessed as "included" for further analysis.

Unnecessary loss of production needs to be highlighted since this loss obtained severity level of damage (2). If only following the severity parameter, the loss should have been screened out. However, the loss was still assessed as "included" due to the first parameter which was analysis objective. The main purpose of SGB is to process the hydrocarbon. The loss was the main concern of the company, as stakeholder, since it might reduce their profit if happened. It was necessary to investigate possible event that may cause loss in the process.

Costly equipment damage was assessed as "included". The loss obtained assessment result (S,K) of (3,3). From knowledge level parameter, it was judged as moderate. No further study was required. From severity parameter, it passed the minimum criteria of major damage due to the consequence it can incur. Additionally, the loss was also inline with the analysis objective which was to analyze the whole SGB system.

None of the identified loss obtained weak knowledge level assessment. No additional process should be performed to the identified loss.

"Screened out" example could not be obtained from the current assessment. It is due to the obtained losses were high level (unrefined) and the analysis was applied to the whole SGB system. If further refinements are made and the analysis is perform for specific system within SGB system, then it is possible to obtain unrelated loss with the system. For example, unnecessary loss of production can be refined into production loss due to inefficient choke valve operation. If the system currently analyzed is the pump system, then the refined loss is irrelevant and should have been screened out from the analysis.

Loss assessment result

The loss severity levels were inherited into the system level hazard with the worst case approach. The system level hazards now contained additional information, that were:

H.1 Pipeline pressure too high (L1, L2, L3) (S4)

H.2 Equipment pressure too high (L1, L2, L3) (S4)

H.3 Equipment pressure too low (L2, L3) (S3)

H.4 Inefficient production process (L3) (S2)

5.3 UCA Screening

A total of 99 UCAs was obtained from basic STPA step 3 in Section 3.4. UCAs were assessed based on four criteria: severity, conditional event likelihood, mitigation possibility and level of knowledge. UCA priority number (UCAPN) for each UCA was calculated from the results. The assessment results were judged against UCA screening criteria in Table 5.2. Screened out UCA were removed from further analysis and recorded for reference.

This section is separated into three subsections: assessment process, screening process and result and discussion. Assessment process discuss the process to assign classification

level for the four criteria. Screening process determine the judgment process for each UCA against the screening criteria. Result and discussion presents UCA screening result and presentation. Additionally, brief discussion on the results are performed.

Assessment process

The assessment process is elaborated from example of the first UCA "operator does not adjust set point of choke valve when the pressure of hydrocarbon in the SGB bypass line is high [H1]". UCA was assessed based on the four criteria: severity, condition event likelihood, mitigation possibility and level of knowledge.

UCA severity level was obtained from system level hazard. The first UCA was linked to hazard H1 "pipeline pressure too high (L1, L2, L3) (S4)". [H1] contained information that the severity level was severe loss (4) which was then inherited to UCA. An explanation could be made to point out the link between UCA, system level hazard and loss. If the increasing pressure was not controlled, then it was plausible that it might lead into overpressure in the pipeline. The worst possible consequence was then pipeline burst which cause environmental pollution. Environmental pollution had been judged earlier as having severe loss (4) severity level. The final assessment of severity level for the first UCA was "severe loss" (4).

Next was to assess the conditional event likelihood of UCA. The conditional event "when the pressure of hydrocarbon in the SGB bypass line is high" was used for assessing the probability of the event to happen. Bypass operation had been initially assumed to take up lower overall operational time than set point adjustment operation. The likelihood of having high pressure in bypass line was lower, because the system was less often in the state of using the bypass line. Therefore, the likelihood of conditional event was assessed as "low".

The UCA was then evaluated based on the mitigation possibility. Two assumptions had been made. The pressure increase was assumed to be fast. Although it reduced the mitigation possibility, automatic control was assumed to be capable of takeover during emergency situation. Therefore, the mitigation possibility was judged to be possible (3).

The assumptions for both conditional event likelihood and mitigation possibility were noted and then measured as the level of knowledge. Due to the several simplifications made in the assumption, the knowledge level was measured as moderate (3).

UCAPN was then calculated by the formula from Equation 4.1. UCA assessment obtained the set (S, L, M, K) of (4, Low, 3, 3). The value of S, M and K were used to calculate UCAPN, obtaining the 36 as the priority number. Based on the priority range on Table 4.10, this UCA had medium priority.

Example of the UCA assessment summary can be seen in Table 5.4.

Screening process

After evaluating the UCA based on all four criteria, the UCA was then screened according to the acceptance criteria. The first UCA obtained low likelihood of conditional event assessment. The minimum passing criteria for UCAPN for low likelihood of conditional event was 15 (see Table 5.2). The UCAPN value obtained from the analysis was 36, higher than the passing grade of 15. Therefore, the first UCA was assessed as "included" for the following analysis.

Table 5.4: UCA Assessment Results Table (Example)

UCA Tag	UCAs	Severity (Worst-Case)	Mitigation	Knowledge	UCAPN	Condition Likelihood	Assumption	Assessment
UCA.OPE.001	Operator does not adjust set point of choke valve when the pressure of hydrocarbon in the SGB bypass line is high [H1]	4	3	3	36	Low	* Automatic control may takeover during emergency * Pressure increases fast	Included
UCA.OPE.003	Operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass line [H1]	4	4	3	48	Low	* Automatic control may takeover during emergency * Pressure increases fast	Included
UCA.OPE.004	Operator reverts the set point of choke valve before the pressure of hydrocarbon in the SGB bypass line return to normal [H1]	4	3	1	12	Low	* Pressure in the process line is still high but already controllable	Screened Out

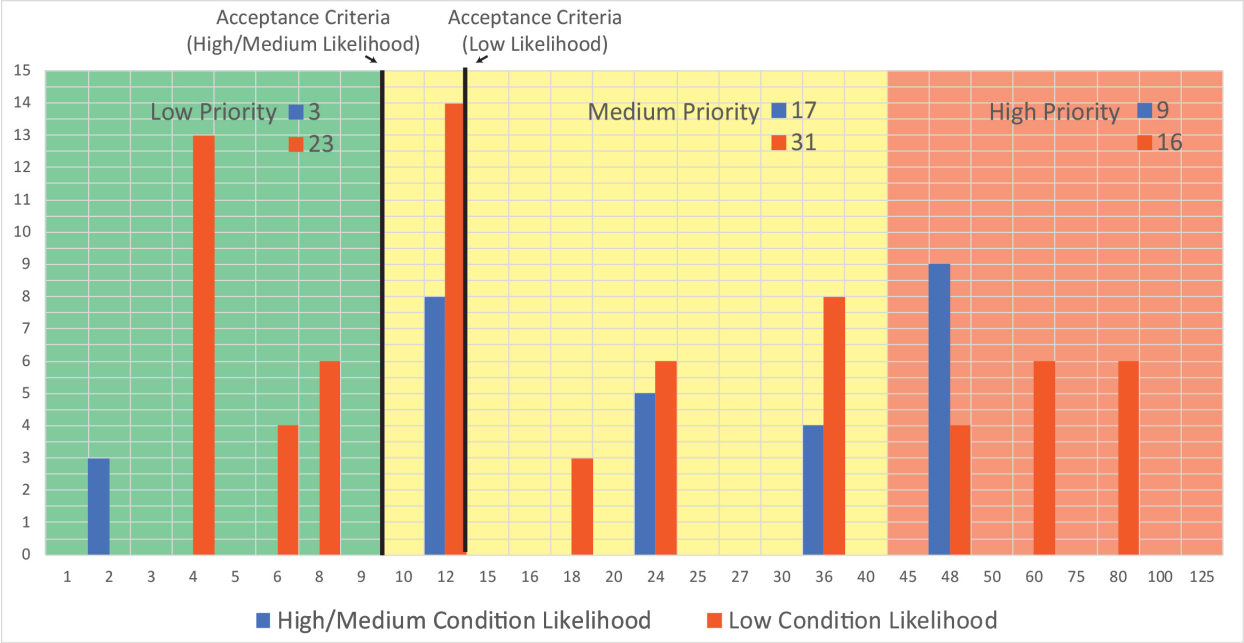


Figure 5.1: UCA Assessment Results Distribution

Another example can be taken from the third UCA "Operator reverts the set point of choke valve before the pressure of hydrocarbon in the SGB bypass line return to normal [H1]". The UCA obtained set result (S, L, M, K) of (4, Low, 3, 1). According to the acceptance criteria, it does not pass the minimum UCAPN value of 15 (UCAPN value is 12). Thus, the UCA was screened out from further analysis.

The only difference between the first UCA and the third UCA was the level of knowledge. It caused different treatment between both UCA (one was included while another was screened out). The latter UCA had higher knowledge level due to the assumption that the process was already controllable. The process was controlled by automatic controller. During this condition, dangerous situation were already happened. Operator should have been more aware of the situation and required to perform a set of procedure before actually able to override automatic controller command and revert set point of choke valve. The assumption was judged as very reasonable and increase the reliability of mitigation possibility assessment result.

Result and discussion

Similar analysis processes were performed to all 99 identified UCAs. The complete list of UCA assessment results can be seen in appendix D.

Table is used to present the summary of assessment result. In the table, tag name is assigned to each UCA. This is to simplify UCA recognition. The tag consist of three parts

$$< UCA > . < Controller > . < Tag\ count >$$

Example is taken to understand the tag meaning. The first UCA had tag name "UCA.OPE.001". It meant that the tag was assigned to the first (001) UCA that happened due to operator (OPE) as the controller. All 99 UCAs were assigned to different tag names with similar format.

The distribution of UCA priority number is presented on Figure 5.1. There were 70 UCAs with low condition likelihood, 10 UCAs with medium condition likelihood and 19 UCAs with

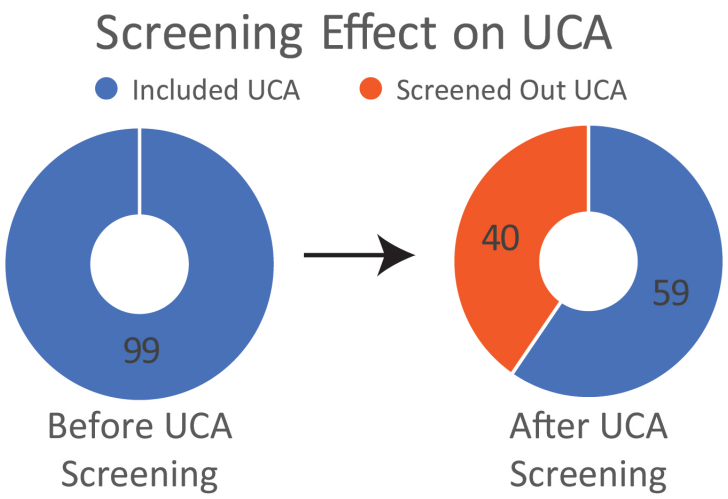


Figure 5.2: UCA Screening Effect

high condition likelihood. The UCAs were distributed on the priority range from table 4.10. There were 26 low priority UCAs, 48 medium priority UCAs and 25 high priority UCAs.

UCA screening criteria from Table 5.2 was used to screen the UCAs. High and medium condition likelihood criteria have minimum UCAPN value of 10. 26 UCAs were included and 3 UCAs were screened out from further analysis. On the other hand, low condition likelihood criteria had minimum UCAPN value of 15. 33 UCAs were included and 46 UCAs were screened out from the analysis. The total UCA screening results were 37 UCAs need to be screened out and only 50 UCAs were included for further analysis (see Figure 5.2). The screened out percentage was rather high (40.40%) due to the optimist approach used in the acceptance criteria.

5.4 Scenario Ranking

A total of 593 scenarios was obtained from basic STPA step 4 in Section 3.5. Only 422 scenarios were refined and fit for the assessment process. Due to UCA screening, scenarios that were supposed to be included for the analysis were further reduced into 219 scenarios. The 203 screened out scenarios were assessed as well for use in latter discussion. The scenario were assessed based on four criteria: severity, likelihood, mitigation possibility and level of knowledge. Although the criteria used were similar to the UCA screening criteria, additional information obtained from loss scenario assessment increased the reliability of likelihood assessment. Due to this, the uncertainty of risk could be reduced. The resulting scenario were ranked in order from high to low, with higher number denotes higher risk.

A total of 42 causal factors had been identified from the scenario. They were summarized in Appendix C. Scenarios that shared the same causal factors were gathered into one and used for ranking of causal factors. The ranking were based on SCRPN value from the scenarios. The results were represented in the hierarchical control structure form for illustration.

This section is separated into three subsections: assessment process, assessment results and discussions and causal factor results and illustration. Assessment process describes the process to obtain the classification level for the four criteria. The results are then presented and discussed in the next subsection. The final subsection presents the link between scenarios and causal factor. Additionally, the result was illustrated into an informative figure for ease of communication between analyst and designer.

Assessment Process

An example from the scenario assessment is explained to illustrate the process. The scenario is "lack of understanding to the appropriate respond when facing the situation". This scenario was linked to the first UCA "operator does not adjust set point of choke valve when the pressure of hydrocarbon in the SGB bypass line is high [H1]". Scenario was assessed based on four criteria: severity, likelihood, mitigation possibility and level of knowledge.

Information about severity, event likelihood, mitigation possibility and UCA level of knowledge were inherited from the first UCA to the selected scenario to obtain set (S, L, M, K) of (4, Low, 3, 3). Further assessments were made for likelihood and level of knowledge.

The scenario likelihood was assessed based on the combined information from both causal factor and conditional event likelihood. For the selected scenario, operator knowledge was the causal factor. It was classified as systematic error since the operator does not have the knowledge due to systematical reason, such as lack of training, etc. The analyst estimated initially that there was possibility (3) for the operator to not have understanding when abrupt situation change. This was due to the assumption that training was inadequate to simulate the actual condition. Operator might commit mistakes during this situation. Although there was possibility (3) to have operator mistake, the conditional event likelihood of the current scenario itself was low. Therefore, the scenario likelihood should be lower and finally assessed as "remote" (2).

Additional information and assumption that were used for assessing the scenario likelihood were recorded and measured for the scenario level of knowledge. In this case, data reference for operational mistake was unavailable. The knowledge level can only be assessed as "weak"(5). Knowledge level of both UCA (3) and from scenario assessment (5) were combined into final scenario level of knowledge by using worst case approach. Since scenario were having weaker knowledge, the uncertainty of the scenario risk, which contain both information, should be higher. This final assessment of scenario knowledge was "weak" (5).

The four criteria was summarized into scenario assessment result set (S, L, M, K) of (4,3,2,5). SCRPN value was then calculated based on the Equation 4.2. The scenario got SCRPN value of 120. According to the risk range on table 4.11, the scenario was classified as having non-tolerable risk.

Example of the unranked scenario assessment summary can be seen in Table 5.5.

Assessment results and discussions

Similar assessment processes were performed to the 422 scenarios, consisting of 219 "included" and 203 "screened out" scenarios. Note that the assessment was not performed to the 171 unrefined scenario due to difficulty to determine the likelihood from the vague scenario. The complete ranked assessment results can be seen in appendix E.

Table is used to present the summary of assessment result. Similar to UCA, tag name is assigned to each scenario. The tag name format is

$$<SCE>.<Controller>.<UCA\ count>.<CF\ type>.<Scenario\ count>$$

Example is taken from the tag SCE.OPE.001.1A1.002 to convey the contained information. The tag indicated that the selected scenario is the second scenario (002) associated with the first UCA (001), which happened due to operator (OPE) as the controller. Additionally, the selected scenario was refined based on the first refinement of causal scenarios type, inappropriate decision (1A1). All 422 scenarios are assigned with different tag name based on the specified format.

Table 5.5: Scenario Assessment Results (Example) (Unranked)

Sce Tag	Scenario	Severity	Mitigation	Condition Likelihood	Scenario Likelihood	UCA Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.001.1A0.001	Operator understand-that there is significant change of pressure of hydrocarbon in the SGB bypass line, but does not provide set point adjustment of choke valve.	4	3	Low	-	3	3	0	* Unrefined scenario
SCE.OPE.001.1A1.002	Lack of understanding to the appropriate respond when facing the situation.	4	3	Low	2	3	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.001.1B1.004	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	4	3	Low	2	3	3	72	* λ = 4,996E-6 (Oreda, 2002, p.811) * T = 10 Year

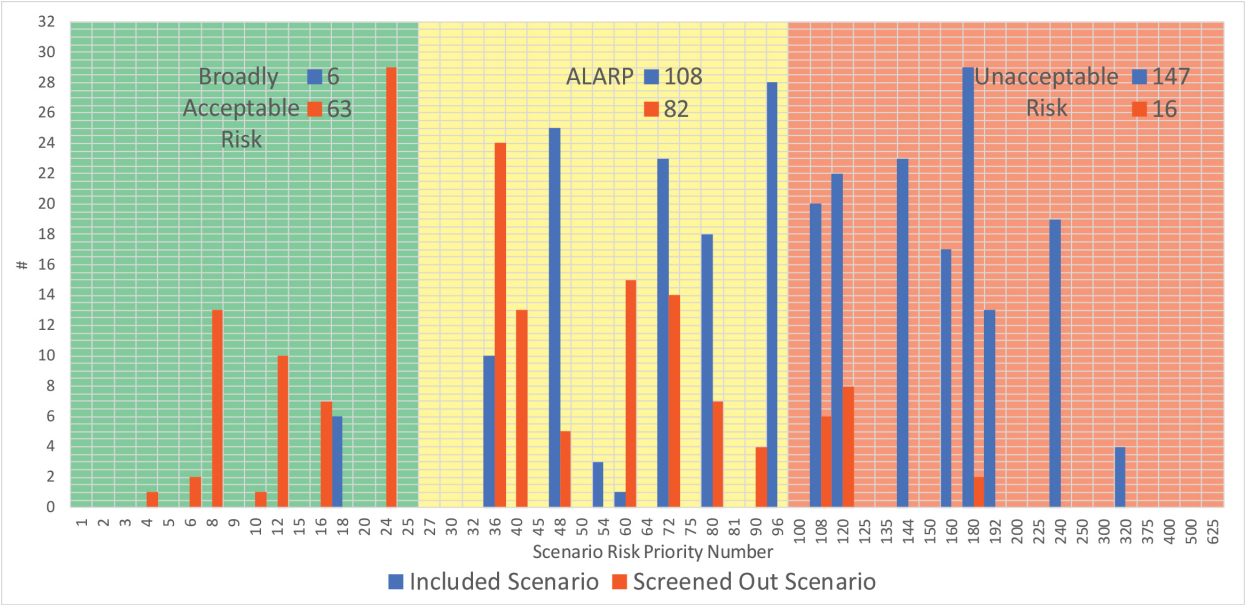


Figure 5.3: Scenario Assessment Results Distribution

The assessment distribution is presented in Figure 5.3. The figure shows that all the included scenarios laid in either ALARP (108 scenarios) or non-tolerable risk (147 scenarios), consistent with the initial hypothesis (see section 5.1). The assessment of screened out scenarios point out that there were 16 scenarios that laid in the non-tolerable risk region with 2 of the scenarios have SCRPN of 180. Additionally, the number of scenarios that laid in the ALARP region were 82 scenarios, quite high number despite the effort made for the assessment. These issue raise question on whether the previous screening process was helpful or not. Possible solution for this issue is to change the initial acceptance criteria to see whether it may affect the results. Tests are performed in the next chapter for detailed discussion.

Causal factor results and illustration

The maximum SCRPN from each scenario was assigned to the linked 42 causal factors. The complete ranked assessment results can be seen in appendix F.

An example is taken to elaborate the result. Causal factor "SCU software setting" setting might cause 57 scenarios, with 25 scenarios out of them are included after UCA screening. Table 5.6 presents the frequency distribution of the causal factor. Although the causal factor has different SCRPN value, it could be argued that when the causal factor happened, the stakeholder want to avoid the worst-case condition. Therefore, it was more appropriate to use the highest SCRPN value since it indicated the highest risk that the causal factor might induce. Therefore, causal factor "SCU software setting" obtained SCRPN value of 320.

The causal factors are presented in the hierarchical control structure in Figure 5.4. The figure illustrates how inadequate design of elements within the control structure might lead into loss causal factor. The causal factor were listed together with their SCRPN value. Therefore, designer will then be able to point out which of the following design issue needs to be solved first when investigating each element.

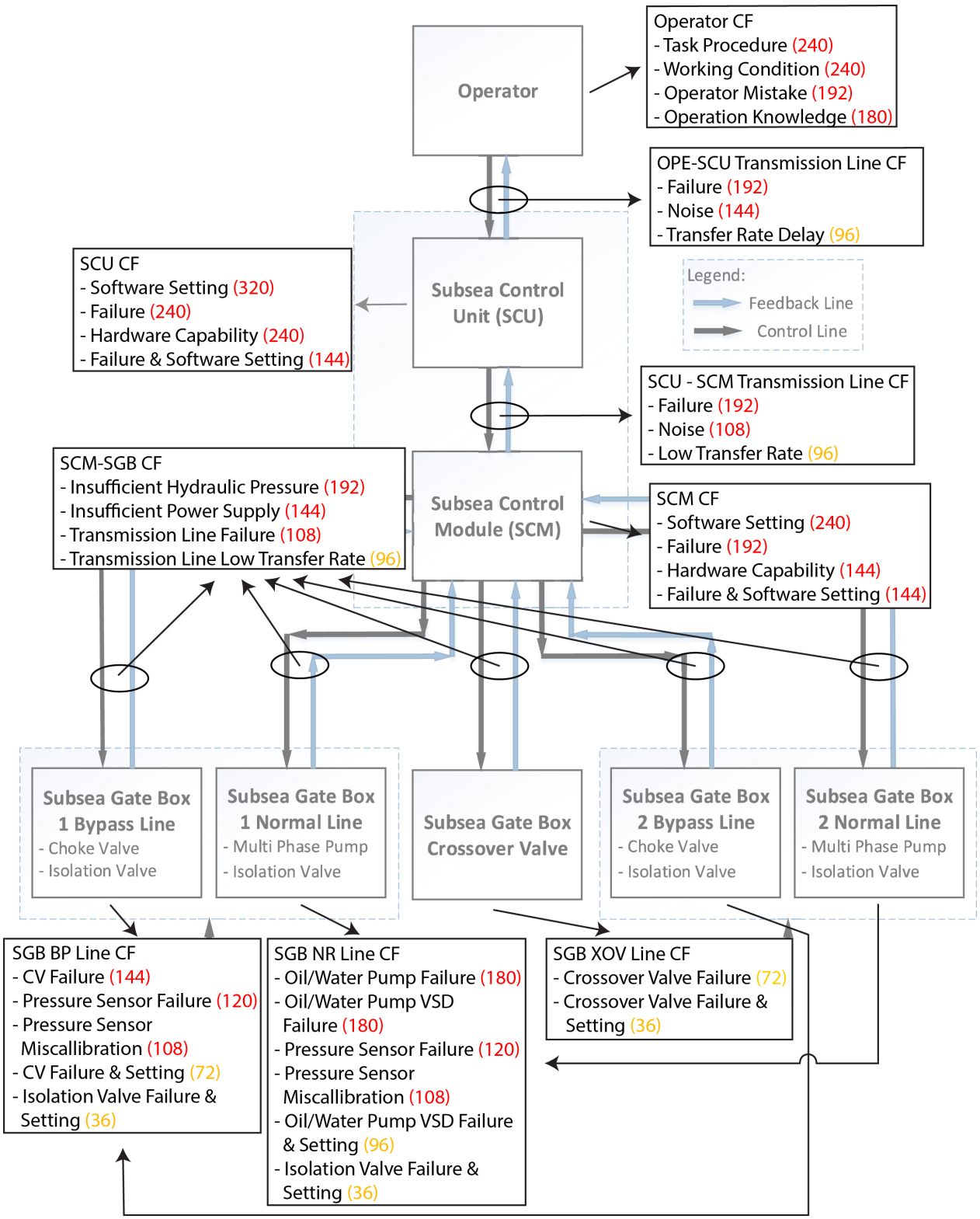


Figure 5.4: Hierarchical Control Structure based on Causal Factor

Table 5.6: Causal Factor "SCU Software Setting" Frequency Distribution

SCRPN Value	Frequency	Note
40	3	All scenarios are screened out from UCA screening
60	11	All scenarios are screened out from UCA screening
90	4	All scenarios are screened out from UCA screening
120	12	All scenarios are screened out from UCA screening
160	3	
180	17	2 scenarios are screened out from UCA screening
240	3	
320	4	

5.5 Solution Priority

Solutions are proposed either to prevent or mitigate the causal factor from causing loss scenario. In the current analysis, the solution recommendation was demonstrated only on one of the causal factor. It is because the process of solution recommendation is brainstorming. Adding the efforts to propose solutions for other causal factors were deemed unworthy. The focus here is rather to show how prioritization can be performed on the recommended solutions.

One causal factor is selected. It is "SCM failure". The causal factor affected 13 scenarios, 9 of which were included from UCA screening, and has maximum SCRPN value of 240. Solutions were required to reduce the risk. Through brainstorming process, two solutions were presented. The possible solutions were either increasing availability requirement for 1oo1 voting SCM or changing SCM voting configuration into 1oo2 with lower availability requirement. Evaluations were made on the two possible solutions.

The solutions were assessed based on three criteria: cost, effectiveness and level of knowledge. Based on calculated solution priority number, the resulting solutions for each causal factor were ranked in order from high to low.

The section is split into two subsections: assessment process and result and discussion. Assessment process elaborates how classification level is assigned to the solution. The result is then presented and discussed briefly in the following subsection.

Assessment process

The assessment process is illustrated for the first solution "higher availability requirement for 1oo1 SCM configuration". Solutions were assessed based on three criteria: cost, effectiveness and level of knowledge.

First the cost was analyzed. The cost required to increase the availability of an equipment were expensive. After a certain point, the required cost were increasing exponentially just to increase the availability by one level. The cost for this solution was assessed as expensive (2).

The solution was then assessed for its effectiveness. Increasing the availability of the equipment proved to be able to reduce the likelihood of failure. However, due to the limited accessibility in the subsea systems, periodical maintenance to help maintain the system risk was not available. Other solution was required to maintain the risk level. Often, the approach used by the company was to replace the SCM after certain period. The provided solution did not prevent the problem effectively. Therefore, the final assessment for effectiveness was "moderate effect" (3).

The assumptions used in both assessment were then recorded. Due to simplifications

Table 5.7: Solution Priority Assessment Results (Example)

CF Tag	Causal Factor	CF Type	Solution	Cost	Effect-iveness	Know-ledge	SOLPN	Assumption
020	SCM failure	Ran-dom	Higher availability requirement for 1oo1 SCM configuration	2	3	3	18	* Limitation on possible availability of controller
			Provide 1oo2 SCM configuration with lower availability requirement	3	3	3	27	* Can still fail due to system-atic error

used in the assumption, the knowledge level of the solution was assessed as "moderate"(3).

Finally, the first solution got set result (C, E, K) of (2, 3, 3). The SOLPN was calculated from the Equation 4.3, yielding SOLPN value of 18.

Result and discussion

Similar assessment was also performed to the second solution "provide 1oo2 SCM configuration with lower availability requirement". The second solution obtained set result of (3, 3, 3), yielding SOLPN value of 27. Table 5.7 summarizes the assessment results.

The SOLPN values were compared between each other. The second solution had higher SOLPN value than the first solution. The only difference between both of them were due to the cost of second solution are lower than the first. The second solution was recommended to the decision maker for final choice.

The same solution priority assessment approach can be performed to all the causal factors. The solutions should be defined first through brainstorming approach before proceeding with the priority assessment.

Chapter 6

Evaluation of PA-STPA

The objective of this chapter is to evaluate the PA-STPA approach. Two approaches are used for the evaluation. First, the PA-STPA results was compared with the basic STPA results. The comparison was judged against two criteria: efficiency and safety. The conclusion of the assessment is discussed in the following subsection. Afterwards, weaknesses of PA-STPA that were identified during the assessment process are discussed further. Readers who are interested to use the proposed approach are recommended to refer to this chapter to understand more about the capability of PA-STPA.

6.1 PA-STPA vs Basic STPA results

6.1.1 Efficiency Comparison

PA-STPA development objective is to propose an approach for prioritizing the STPA results. Additional steps are added in PA-STPA. These additional steps can increase/decrease the efficiency of analysis.

There are two definitions of efficiency that follow the application of STPA: assessment process efficiency and decision making efficiency.

First, the efficiency of the analysis. it refers to the overall increase / decrease of required resource and time that can occur during application of STPA. PA-STPA follows basic STPA process with several additional steps for prioritization approach. Screening is performed to the losses (optional) and UCAs to reduce the amount of considered scenarios in the following assessment. Although these activities reduce the required resource and time and increase the assessment process efficiency, additional required assessment process may lessen the effect.

Second definition, is the efficiency of decision maker to make choice. STPA results are presented to the decision maker for decision making. Basic STPA produces set of scenarios and controller constraints as the result. Decision maker is required to make decisions based on these unranked results. For comparison, PA STPA step 4 and 5 produce ranked scenarios and solutions. These PA-STPA results are able to reduce time required for decision maker to make final choice. Additionally, the reasoning and assumptions are well documented to support the results. These activities increase the efficiency of decision making process.

In this section, the efficiency term that is discussed is for the first definition. The comparison is only performed up to STPA step 4, where the number of main steps between basic STPA and PA-STPA application are equal and comparable. Both results were judged against required resource and time (in man-hours) as analysis parameter for efficiency criterion.

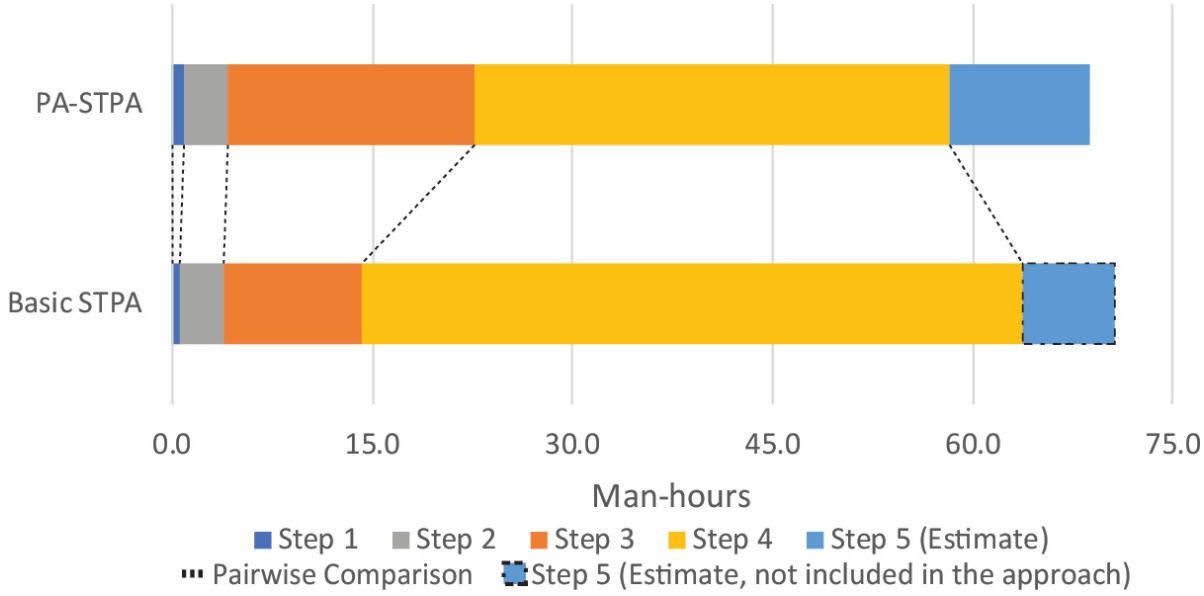


Figure 6.1: Required Time for SGB Analysis: Basic STPA vs PA-STPA

For the second definition of efficiency, it is apparent that ranked results from PA-STPA are easier to be used than unranked results from basic STPA process. Decision maker can make choice relatively more easy if the proposed solutions are ranked and the assumptions for reference are recorded. No further discussion is required.

This section is further split into two subsections: comparison result and discussions and effect of UCA screening criteria on efficiency. The first subsection discuss the results of comparison between both STPA approach based on each main STPA step. The discussion is mainly from PA-STPA point of view since it encompass both basic STPA process and the addition of prioritization approach. UCA screening was identified as the main cause of increase / decrease in analysis efficiency of PA-STPA. Tests to verify the claim were performed and discussed in the latter subsection.

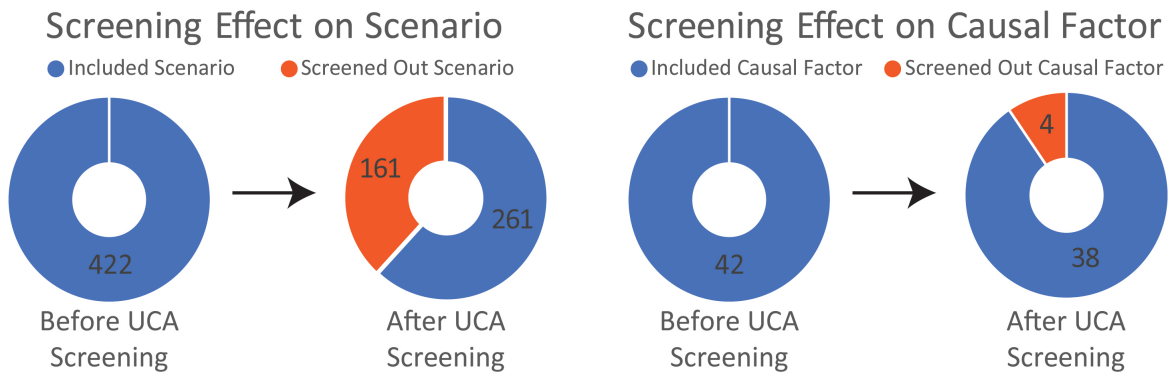
Comparison result and discussions

During PA-STPA step 1, assessments were performed to the losses. A total of three losses were assessed in this step. Due to low number of assessed loss, slight increase in required resource and time occurred. Compared to basic STPA process, PA-STPA required slightly more resource and time.

STPA step 2 process for both PA-STPA and basic STPA are identical. The required resource and time between both STPA approach during this step were equal.

A total of 99 identified UCAs were assessed against four criteria during PA-STPA step 3. Additionally, UCA screening was performed to all UCAs. PA-STPA required more resource and time than basic STPA during this step due to the additional assessment and screening process,.

During PA-STPA step 4, the identified scenarios were assessed and ranked. UCA screening in PA-STPA step 3 managed to reduce the number of included UCA by 40.40% (40 screened out UCAs). In average, UCAs might produce around ≈ 4 loss scenarios. Due to screening effect, the number of scenarios that need to be assessed is reduced into only 261 out of the original 422 refined scenarios produced by basic STPA process. The process reduces the number of scenario by 38.15%, quite similar with the percentage of reduced UCAs (40.40%). PA-STPA had higher analysis efficiency compared to basic STPA in this step.



(a) on Scenarios (b) on Causal Factors

Figure 6.2: UCA Screening Effect on STPA Results

Unrelated to the current comparison process, another point of view can be taken for the screening effect to the causal factor. The reduction effect from UCA screening was only 9.5% (4 screened out causal factors). The reason of this effect are due to the small and interlinked number of elements within SGB system. For example, the elements with the highest number of causal factor is SGB normal line (see Figure 5.4). SGB normal line consists of 2 main component and several smaller components. Since possible interaction within the element itself is high, the number of possible design issues in SGB normal line will be obviously becomes higher than other elements. Although PA-STPA analysis of SGB produces high number of UCAs and scenarios, most of them are caused by similar elements within the system. If the considered elements are expanded, then naturally the number of causal factors will also increases as well. However this effect was not reflected in the current assessment process since the increase of analysis efficiency will take place during PA-STPA step 5.

According to the overall analysis efficiency comparison between PA-STPA and basic STPA process. It is concluded that, for SGB system, PA-STPA manages to increase the efficiency of the process. The increase of analysis efficiency was greatly affected by the reduction on number of analyzed scenarios during PA-STPA step 4.

The summary of efficiency assessment can be seen in Figure 6.1. An illustration is also given for the estimation required resource and time during STPA step 5. The result is not discussed further since the data was only an assumption for both approach.

UCA screening was identified as the main reason of the reduction effect. Figure 6.2 illustrates the effect of UCA screening to both scenarios and causal factors. The different magnitude of effect between scenarios and causal factors were because a lot of scenarios shared similar causal factor. The screened out causal factor were linked to small part out of 161 scenarios that were screened out completely. If the causal factors were linked to scenarios that were both included and screened out, those causal factors were still included for the following analysis.

Effect of UCA screening criteria on efficiency

The original UCA screening acceptance criteria from Table 5.2 was defined as case 0. Three test cases were prepared in addition to examine the effect of UCA screening criteria on assessment process efficiency. The acceptance criteria in these three cases followed the first approach, only considering the UCAPN value as the parameter (see section 4.4.2 step 3.4). Three values of UCAPN were used as the passing criteria: $\geq 10, \geq 5$ and ≥ 15. The first two cases used more conservative approach than case 0. The latter case had the highest passing

Table 6.1: UCA Screening Effect with Various Acceptance Criteria

Type	Case 0 (combined parameter)	(%)	Case 1 (UCAPN >10)	(%)	Case 2 (UCAPN >5)	(%)	Case 3 (UCAPN >15)	(%)
Included UCA	59	59.60	73	73.74	83	83.84	51	51.52
Screened out UCA	40	40.40	26	26.26	16	16.16	48	48.48
Included scenario	261	61.85	309	73.22	354	83.89	227	53.79
Screened out scenario	161	38.15	113	26.78	68	16.11	195	46.21
Included causal factor	38	90.48	42	100.00	42	100.00	33	78.57
Screened out causal factor	4	9.52	0	0.00	0	0.00	9	21.43

criteria out of all the test cases.

Summary of test results is presented in Table 6.1. The assessment process efficiency for the four cases, listed in order of high to low, is case 3 > case 0 > case 1 > case 2. The results indicate that reducing the passing grade parameter also reduce the efficiency of the analysis. For example in the second case, which had the lowest UCAPN passing grade, the screening parameter managed to screen out 16.16% of the overall UCAs and 16.11% of the overall scenarios. These screened out percentage in the second case were the lowest of all the four test cases.

It should be noted that for scenario 1 and 2, the screened out percentage for causal factor is the same 0%. Additionally for all four cases, the magnitude of screened out effect for causal factors are different to the effect on UCAs and scenarios respective to each case. For example in case 3, the percentage of screened out UCAs and scenarios are almost the same (48.48% and 46.21%). Compared to the causal factor, the screened out percentage is lower, only 21.43%. They occurred due to the high level definition of causal factor produced by the analysis. This high level definition limited the amount of possible design problems related to each element in the control structure. A lot of scenarios were classified under similar causal factor, masking the actual effect of analysis efficiency in STPA step 4. As discussed in the previous subsection, the increase of efficiency due to causal factor reduction is applicable only on PA-STPA step 5. The increase of efficiency in PA-STPA step 5 cannot be compared to basic STPA process since on the latter process, the analysis stops after scenario had been identified. No solutions are produced from basic STPA process. Better comparison of the efficiency effect should be inferred from the amount of screened out UCAs and scenarios that take place during STPA step 4.

Table 6.2: Causal Factor with Hidden Risk

CF Tag	Causal Factor	Included Scenario	Max SCRPN	Screened Out Scenario	Max SCRPN
027	SCU software setting	25	320	32	180
042	Working condition	9	240	3	80
029	Transmission line HMI - SCU failure	13	192	10	108
036	Transmission line SCU - SCM failure	7	192	5	108
018	Operator knowledge	14	180	25	120
023	SCM software setting	9	144	10	72
025	SCU failure & software setting	2	144	6	108
030	Transmission line HMI - SCU Noise	2	144	17	72
037	Transmission line SCU - SCM Noise	7	108	5	108
001	BP line isolation valve (XV-002 / XV-004) failure	0	0	2	72
012	NR line isolation valve (XV-003 / XV-005) failure	0	0	2	72
034	Transmission line SCM - SGB Noise	0	0	2	72

6.1.2 Safety Comparison

Prioritization approach has been developed to increase the efficiency of analysis, both in the analysis and in decision making process. However, the increase of efficiency in the analysis process comes together with reduction in the completeness of analysis results. This reduction raises argument whether the results still conform with the required system safety or not. It should not be forgotten that the main reason of performing hazard analysis is to achieve safety by identifying hazardous events and scenarios that cause loss.

Comparison was performed between both STPA approaches based on safety criteria to determine whether the increase in efficiency compromises system safety. The safety of STPA results is judged qualitatively against the risk as parameter. Since the reduction occurred during PA-STPA process, risk values obtained from the assessments were used as basis for discussion.

This section is further split into two subsections: comparison result and discussion and effect of UCA screening criteria on system safety. Result of comparison between both STPA approaches are presented and discussed in the first subsection. UCA screening was identified to cause the reduction of analysis completeness in the PA-STPA approach. Safety level of the PA-STPA results can be arguably maintained at the same level if the risks of the screened out scenario lay in the broadly acceptable region. Tests were performed to prove the effect of screening on system risk. The results were discussed in the latter subsection.

Comparison result and discussions

It has been mentioned before in Section 5.4 and illustrated in Figure 5.3 that there are several screened out scenarios that lays in unacceptable (21 scenarios) and ALARP (113 scenarios) risk region. These results were alarming since they indicate that, for some scenarios, the increase in analysis efficiency is achieved by compromising safety.

Another look was taken from causal factor point of view. Table 6.2 presented the list of hidden risk in causal factor. Most of the scenarios with unacceptable risk were due to

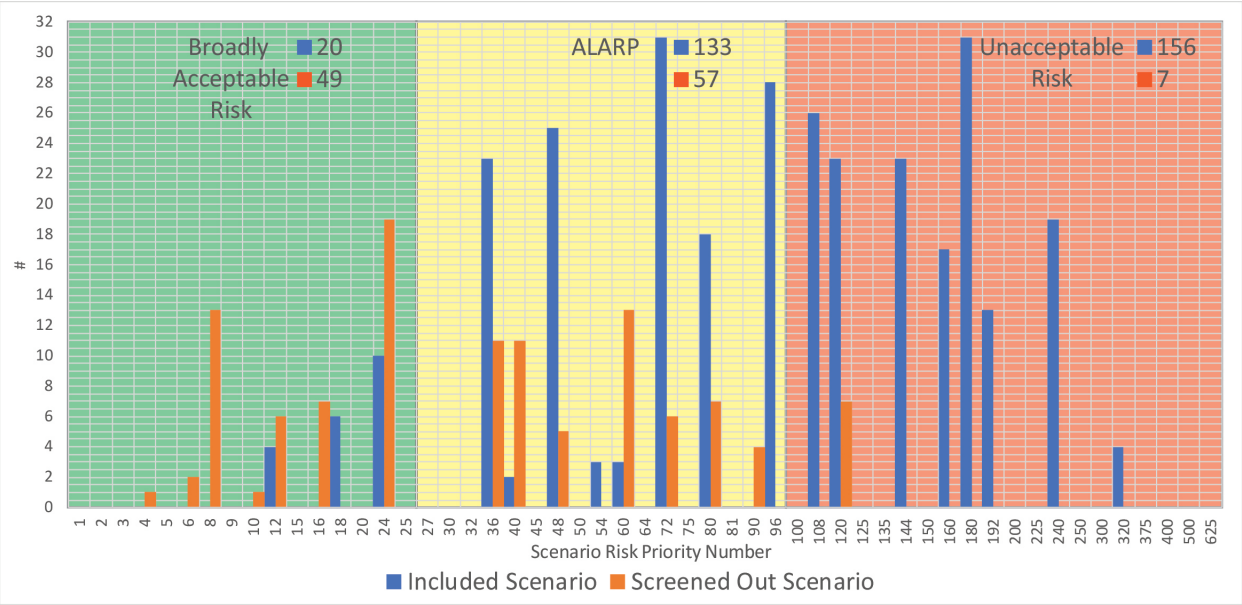


Figure 6.3: Scenario Assessment Results Distribution for Case 1 (Screening Criteria UCAPN > 10)

several causal factors with higher likelihood of failure and lower level of knowledge. Though the scenario are originally filtered in UCA screening due to low UCAPN value, the SCRPN value might increases greatly due to the addition of likelihood criteria in the formula and the updated value for level of knowledge. For example, the UCAPN value of UCA "SCM gives incorrect signal during SCU command to open normal line isolation valve (XV-003 / XV-004) [H1, H2, H4]" is 12. This value was obtained from set (S, L, M, K) of (4, Low, 3, 1). According to UCA screening criteria in Table 5.2, this UCA should be screened out from the analysis. However, from basic STPA process, it had been identified that one possible loss scenario to this UCA is caused by "SCU software setting". This causal factor from the assessment increase scenario likelihood to possible (3) and updated level of knowledge becomes weak (5). The scenario obtained set (S, L, M, K) of (4, 3, 3, 5), resulting into SCRPN value of 180. The process shows how UCAs with low UCAPN values manage to have high risk in the latter part.

The ideal expectation from PA-STPA process is that the safety level should be maintained throughout the process. When the UCAs are being screened out, two possible options should have happened. First, the UCA is presumably truly has low risk level. Second, if the actual risk is high, then it is expected that it is caused by similar causal factor that is not screened out yet (as seen in Table 6.2 for CF 018, 023, 025, 027, 029, 030, 036, 037 and 042). However, causal factor 001, 012 and 034 proved otherwise. UCA screening managed to screened out scenarios that were supposed to lay in the ALARP region (SCRPN value of 72). For some scenarios, the PA-STPA process had compromised system safety to achieve more efficient process.

Effect of UCA screening criteria on system safety

Similar test cases to the one performed in Section 6.1.1 had been prepared. In total, there are four cases that were compared between each other based on completeness and risk value.

An example can be taken from case 1. Table 6.3 presents the result of UCA screening on

Table 6.3: Scenario Risk with Various Acceptance Criteria

Scenario Type (Risk Region)	Case 0 (combined parameter	Max SC-RPN	Case 1 (UCAPN >10)	Max SC-RPN	Case 2 (UCAPN >5)	Max SC-RPN	Case 3 (UCAPN >15)	Max SC-RPN
Included (unacceptable)	147	320	156	320	163	320	124	320
Screened out (unacceptable)	16	180	7	120	0	-	39	240
Included (ALARP)	108	96	133	96	159	96	97	96
Screened out (ALARP)	82	90	57	90	31	60	93	90
Included (broadly acceptable)	6	18	20	24	32	24	6	18
Screened out (broadly acceptable)	63	24	49	24	37	24	63	24
Total included scenario	261	N/A	309	N/A	354	N/A	227	N/A
Total screened out scenario	161	N/A	113	N/A	68	N/A	195	N/A

the risk of included / screened out scenario. The maximum SCRPN value for screened out scenario in the unacceptable region is 120. Compared to case 0 (refer to Figure 5.3), the maximum risk of screened out scenario decreases by 60 points. Additionally, the SCRPN value of screened out scenario in ALARP region decreases by 6 point (from 96 to 90). Although the reduction is minimal, based on this comparison, lower passing grade for acceptance criteria will also decrease the risk of the screened out scenarios.

To support the claim, another example is taken from screened out scenarios in the unacceptable range. Comparatively, both number of screened out scenarios and maximum risk for the screened out scenario decreased in order from case 3 (39 scenarios, 240 max SCRPN) > case 0 (16 scenarios, 180 max SCRPN) > case 1 (7 scenarios, 120 max SCRPN) and case 2 (0 scenarios, not applicable max SCRPN). This result indicates that lower acceptance criteria can reduce the possibility of screening out higher number of scenarios with high risk.

Similar comparison can be performed for screened out scenario in the ALARP region. Although the maximum SCRPN values for case 0, 1 and 3 are equal (90), the number of scenario that should be screened out are different. The criteria affect the number of screened out scenario differently. Case 0, 1 and 3 have 82, 57 and 93 screened out scenarios respectively. Lower number of screened out scenarios means that the amount of scenario with 90 SCRPN values should be lower as well. Lower acceptance criteria are still capable to reduce the risk of screening out more scenarios with high risk.

A summary of screening effect based on different screening criteria on the scenario risk are presented in Table 6.3. Although the table cannot illustrate the actual distribution within the result as clear as what Figure 5.3 and 6.3 give, the maximum risk within each region can still represent the effect of screening on scenario risk. The test results indicates that more conservative approaches manage to increase system safety. It is shown from the reduction of

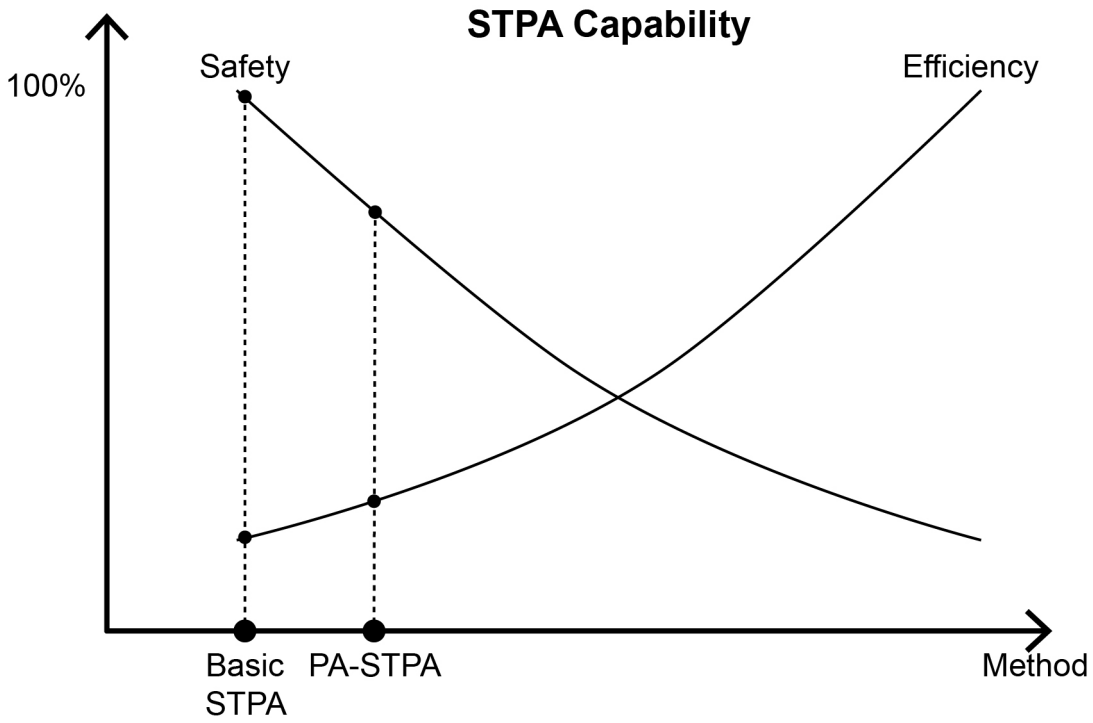


Figure 6.4: Capability of PA-STPA & Basic STPA

maximum SCRPN value of the screened out scenarios for case with lower value of screening criteria. It can be concluded that using more conservative approach to define the screening criteria not only increases the analysis completeness, but also reduce the risk of screening out high-risk scenario.

6.1.3 Comparison Conclusion

Comparison had been performed for both STPA process against two criteria: efficiency and safety. Based on the results, it can be concluded that PA-STPA is capable to increase the overall analysis efficiency, while having possibility to screen out high-risk scenarios. This claim is only based on the application of both approaches on SGB system. The effect may differs from one system to another.

In addition, the main cause that change the effect of efficiency and safety had been identified. UCA screening criteria is the main contributor of the change. More conservative acceptance criteria should be used to prevent the screening of high-risk scenarios. Figure 6.4 illustrates the capability of PA-STPA compared to basic STPA process. The capability of both STPA approach are not fixed, like shown the figure. Different factors may contribute with the effect of change. For example, the level of detail and scope of analysis contributes to the efficiency and safety of basic STPA application. While for PA-STPA, UCA screening criteria also contributes to the capability change together with both level of detail and analysis scope.

Specific to PA-STPA, the condition likelihood information from PA-STPA step 3 should be used cautiously. Discussion in Section 5.3 shows that this criteria increased complexity of screening parameter. It has been proven as well from discussion in Section 6.1.1 that the approach of having higher passing grade for UCA screening also contributes to the reduction of safety level. It may screened out scenario with higher risk. Using single parameter UCAPN is a better alternative to simplify UCA screening process.

PA-STPA provides better option than basic STPA approach since it increases the efficiency of both analysis process and for the decision making. However, the approach should be used with caution. Conservative approach for UCA screening criteria assignment should be used in order to reduce the risk of screening out high-risk scenario.

6.2 Weakness of PA-STPA

Through analysis process and several tests, several weaknesses of current PA-STPA process had been identified. The weaknesses are subjectivity of the assessment, formula used for calculation, and results safety issue. The following sections discuss thoroughly for each weakness.

6.2.1 Subjectivity of the Assessment

Qualitative assessment is inseparable with subjective judgment. It is because the description of each class is vague and the result does not have exact value as what quantitative calculation could provide. Analyst may have differed opinion even if the data and assumptions used are the same.

An example is taken for analysis of scenario with causal factor "operator knowledge". Likelihood assessment was performed to the selected causal factor. Operator knowledge was a systematic problem. The acquired frequency, if any, could not be easily justified. Multiple conditions and simplification could affect the judgment of operator. Bayesian approach was then used to assess the likelihood. The assumption used in the current approach was "probability of operator inability to perform, given required knowledge is not available". In addition to that, the analyst used additional assumption based on their inner assumption and experience. Optimist analysts may consider that the likelihood value as remote (2). Differently, pessimist analysts do the analysis more cautiously. They may assigned higher likelihood value for the operator knowledge as possible (3). If the assumptions used for the analysis are not recorded clearly, the assessment result may become questionable for the reader. The differences in the obtained assessment change the risk value for the scenario affected by the selected causal factor and also affect the overall scenario risk ranking.

Systematic approach has been defined to minimize the effect of subjectivity when developing PA-STPA. During each assessment process, the assumptions used are supposed to be recorded separately. This information is used to inform the reader how the thinking process to obtain the assessed value. Although it is still subjective, the uncertainty range for each assessment can be obtained from the information.

Uncertainty within each assessment is characterized by using the level of knowledge criterion. The knowledge level criterion is used during assessment of UCA, scenario and solution. The recorded assumptions were judged against several descriptions within each class of knowledge level (refer to Table 4.9). Knowledge level criterion help contributes to reduction of subjectivity by changing the resulting calculated priority, risk and benefit. An example is taken from two sets of data from assessment (S, L, M) of (4, 3, 2) and (3, 2, 4). If the formula used for calculation, using Equation 4.3 as reference, while removing K from the formula, both scenario will have the same calculated number 24. Adding knowledge level at this point increase the reliability of assessment since the analyst may have different uncertainty to his assigned number due to use of assumptions. Additional assessments reveal that the set data now become (S, L, M, K) of (4, 3, 2, 3) and (3, 2, 4, 5). Inputting the value into Equation 4.3 reveals that the risk between two data sets are now different. Second data

set have higher risk (120) than the first data (72). This final value informed that the first data set used more assumptions or crude simplifications which makes the assigned number less reliable. Higher priority should be assigned to the second data.

For conclusion, attempt to reduce the subjectivity has been performed by defining systematic approach and include level of knowledge to characterize uncertainty within each assessment. The analysis results are arguably better with the addition of these two approaches. However, it cannot remove the hidden subjectivity within each assessment process completely. The decision maker should be informed with these danger before proceeding to make decision.

6.2.2 Formula for Calculation

RPN calculation formula is adopted for the calculation of UCAPN, SCRPN and SOLPN. It has been discussed before in Section 4.2.3 that RPN has one major weakness which is due to its use of ordinal measurement for calculation. The weakness of RPN is carried over as the current weakness of the PA -STPA.

It is evident that calculated results were capable to inform which of the UCA, scenario and / or solutions had better priority compared to the other. Though the demonstration presented in previous chapter proved the usefulness of the approach, the results validity is still questionable. Therefore, the focus is not to remove the calculation formula, but rather to find out what kind of approach is required to improve the reliability of the result.

Several approaches have been developed as an alternative to replace RPN approach: SOD code (Wheeler, 2011), fuzzy approach (Pelaez and Bowles, 1994; Papic and Aronov, 1996; Moss and Woodhouse, 1999; Chang et al., 1999) and multi criteria decision making (MCDM) (Braglia, 2000; Davidson and Labib, 2003; Chen, 2007). SOD code implements three digit code for severity, occurence and detectability and placed it in order to get the priority number. Fuzzy approach used the defines linguistic terms manipulated by fuzzy logic to determine the priority. MCDM use pairwise comparison within failure modes to determine the importance.

Those approaches are not without weakness on their own. In the first approach, the order of SOD code limit the contribution of the other criteria to the priority result. For example, a failure mode with severity of 3 will always have lower priority than failure mode with severity of 4, despite the likelihood of occurrences. For example, SOD code of 351 will always have lower rank either than 411. From simple logical reasoning, the former SOD code should have higher priority than the latter code. Thus, the reliability of the result become more questionable.

Second, fuzzy approach requires to define set of linguistic terms to be used in the fuzzy logic. Braglia and Bevilacqua (2000) questioned the practicality of the approach. The process is complex and requires considerable time to perform, especially when extensive test of fuzzy rules is required to validate the results.

Third, MCDM approach such as analytic hierarchy process (AHP) have to identify the pairwise comparison within each failure modes. The results of each failure mode can be compared between each other. However, the number of defined pairwise comparison is numerous and the comparison still cannot remove the use of subjective judgment when assigning the pairwise comparison value.

The discussed weakness shows that the development of alternatives for RPN is still an open research that needs to be investigated. As of now, PA-STPA have benefited with the use of RPN approach. Further research should be performed to improve the reliability of results.

6.2.3 Results Safety Issue

Safety issue has been previously discussed extensively in Section 6.1.2 and 6.1.3. From the conclusion, PA-STPA attempts to increase the analysis efficiency is performed by screening of UCA. Screening process increases the possibility of removing scenario with high risk level. To reduce the effect, the criteria used during UCA screening should be lowered. This attempt ensures that high level risk scenarios are still included for the following analysis.

Chapter 7

Summary and Recommendations for Further Work

This last chapter objective is to present the conclusion of the research and discuss recommendation for further works. First summary and conclusion of what have been performed throughout the report is presented. Afterwards, discussions of the findings and possible paths for further work are presented at the latter section.

7.1 Summary and Conclusion

Hazard analysis using systems theoretic process analysis (STPA) is capable to identify numerous amount of possible scenarios and constraints to prevent losses. Although these are typical to all other hazard analysis tools, prioritization approach to rank the produced results have yet to be implemented to STPA. A research to develop a prioritization approach for STPA had been performed and discussed in this report.

Risk-based decision making (RBDM) approach had been identified as the most suitable approach for prioritizing STPA results. Criteria used for prioritization are severity, likelihood, mitigation possibility, cost, effectiveness and level of knowledge. The criteria were assessed for suitability to be used according to each main step of STPA.

Prioritization approach for systems-theoretic process analysis (PA-STPA) is proposed as the RBDM approach for STPA. With basic STPA process as the basis, PA-STPA extends the process with the addition of main step to propose solution based on the scenario. Additionally for prioritization, several processes are added: loss assessment, UCA screening, scenario ranking and solution priority.

PA-STPA application to subsea gate box systems had been demonstrated. A total of 3 losses, 99 UCAs, 422 scenarios (219 "included" and 203 "screened out scenarios) and 2 solutions had been assessed based on PA-STPA approach. PA-STPA is capable to produce prioritized results based on the defined criteria.

Evaluations had been made to compare between basic STPA and PA-STPA results. They were judged against two criteria: efficiency and safety. The comparison found out that the overall analysis efficiency of PA-STPA is better, while having risk of screening out high-risk scenarios. Additional test showed that UCA screening criteria is the main cause of change in the efficiency and safety of PA-STPA application.

Several weaknesses of PA-STPA had been identified. They are subjectivity of the assessment, formula used for calculation and result safety issue. Several countermeasures had been developed and discussed to resolve these weaknesses. Specific to the formula used for

calculation, additional research is required since the identified alternatives still have practical challenge.

7.2 Discussion

PA-STPA has been proposed with system in early design phase as the basis. Though it can be applied as well for system during later design, the approach has yet been tested. There are several differences between application of hazard analysis in both phase, such as analysis objective and detailed system information. Refinements are required to tailor the approach for the system during later design phase.

The comparison of basic STPA and PA-STPA results is objective within the boundary of SGB system analysis results. Several claims made in this research are possibly not applicable for other systems. Readers should use the research result with more caution.

In addition with the identified weaknesses, additional weakness of STPA in general had been identified. The approach does not define how solutions can be generated based on the loss scenarios and / or constraints. Brainstorming approach is used. Although it is applicable, the completeness of the identified solutions are questionable. Often, it is limited by the experience and background of the analyst.

7.3 Recommendation for Further Works

The research is far from perfect, further works are required to improve the result. Several options are available to develop the research.

First, formula used for calculation can be improved. Several alternative approaches have been identified. Although it can be useful, the approaches still have weaknesses on their own. The complexity of approach and validity of the calculated result should be the main basis of improvements.

Second, the approach should be tested for other systems to demonstrate the practicability and prove the claims made in the current research. PA-STPA is developed with system during early design phase as the basis. Additionally, it is currently has been applied only to subsea system. Different results can be produced when the approach is tested to other systems and at different development stage.

Third, for STPA in general, approach to propose solution should be formalized. The current brainstorming approach have limited scope of results. Systematic approach for solution proposal can be considered as it will increase the completeness of proposed solutions.

Appendix A

Acronyms

AHP Analytical Hierarchy Process

ALARA As Low As Reasonably Achievable

ALARP As Low As Reasonably Practicable

C Cost

CAPEX Capital Expenditure

CC Controller Constraints

CF Causal Factor

DNV-GL Det Norske Veritas Germanischer Lloyd

E Effectiveness

EPU Electronic Power Unit

ESD Emergency Shutdown System

FMECA Failure Mode Effect and Criticality Analysis

GAMAB Globalement Au Moins Aussi Bon

HAZOP Hazard and Operability study

HMI Human Machine Interface

HPU Hydraulic Power Unit

K Level of Knowledge

L Likelihood

M Mitigation Possibility

MCDM Multi Criteria Decision Making

MP Multiphase

NTNU Norges Teknisk-Naturvitenskapelige Universitet

O Occurrence

OPEX Operational Expenditure

PA-STPA Prioritization Approach for Systems-Theoretic Process Analysis

PHA Preliminary Hazard Analysis

PRA Probabilistic Risk Analysis

PSA Probabilistic Safety Analysis

RAMS Reliability, Availability, Maintainability, and Safety

RBDM Risk-Based Decision Making

RIDM Risk-Informed Decision Making

RPN Risk Priority Number

S Severity

SC Safety Constraints

SCM Subsea Control Module

SCRPN Scenario Risk Priority Number

SCU Subsea Control Unit

SGB Subsea Gate Box

SOD Severity, Occurrence, Detectability

SOLPN Solution Priority Number

STAMP Systems-Theoretic Accident Model and Processes

STPA Systems-Theoretic Process Analysis

SUBPRO Subsea Production and Processing

UCAPN UCA Priority Number

UCAs Unsafe Control Actions

Appendix B

Controller Details

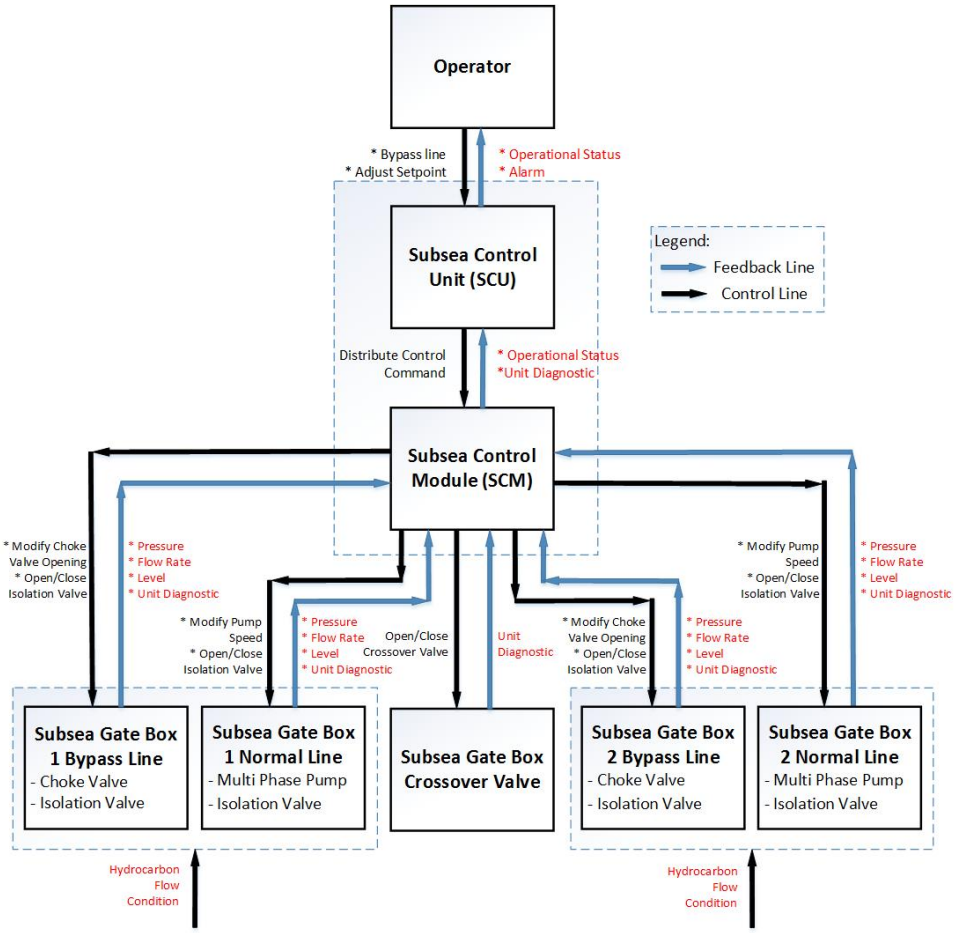


Figure B.1: Subsea Gate Box Hierarchical Safety Control Structure

This section describes the control actions and feedback received for each controller. This feedback information is then checked with the process model of the controller to determine the control action. The detailed control structure can be seen in Figure B.1.

Operator

Table B.1: Control Actions for Loop Operator – SCU

Control Action	Given To	Description
Adjust Set Point of Choke Valve	Subsea Control Unit (SCU)	Choke valve set point is adjusted to regulate the downstream pressure
Adjust Set Point of Oil MP Pump Speed	Subsea Control Unit (SCU)	Minimum pressure should be achieved by the oil to flow to topside
Adjust Set Point of Water MP Pump Speed	Subsea Control Unit (SCU)	Minimum pressure should be achieved by the water to flow to topside
Change Flow Line, SGB1 Normal ->SGB1 Bypass	Subsea Control Unit (SCU)	In case of failure in SGB1 normal line, it is possible to reroute the flow to SGB1 bypass line. Priority for efficiency should be considered
Change Flow Line, SGB1 Normal ->SGB2 Normal	Subsea Control Unit (SCU)	In case of failure in SGB1 normal line, it is possible to reroute the flow to SGB2 normal line. Priority for efficiency should be considered
Change Flow Line, SGB1 Normal ->SGB2 Bypass	Subsea Control Unit (SCU)	In case of failure in SGB1 normal line, it is possible to reroute the flow to SGB2 bypass line. Priority for efficiency should be considered
Change Flow Line, SGB1 Bypass ->SGB1 Normal	Subsea Control Unit (SCU)	In case of failure in SGB1 bypass line, it is possible to reroute the flow to SGB1 normal line. Priority for efficiency should be considered
Change Flow Line, SGB1 Bypass ->SGB2 Normal	Subsea Control Unit (SCU)	In case of failure in SGB1 bypass line, it is possible to reroute the flow to SGB2 normal line. Priority for efficiency should be considered
Change Flow Line, SGB1 Bypass ->SGB2 Bypass	Subsea Control Unit (SCU)	In case of failure in SGB1 bypass line, it is possible to reroute the flow to SGB2 bypass line. Priority for efficiency should be considered

Table B.2: Feedback for Loop Operator – SCU

Feedback	Received From	Description
Bypass line hydrocarbon pressure	Subsea Control Unit (SCU)	Pressure condition in the bypass process line
Separator Pressure	Subsea Control Unit (SCU)	Separator tank inside pressure
Oil MP Pump Differential Pressure	Subsea Control Unit (SCU)	The differences between outlet and inlet pressure of the Oil MP Pump
Water MP Pump Differential Pressure	Subsea Control Unit (SCU)	The differences between outlet and inlet pressure of the Water MP Pump
Flow Route Indicator	Subsea Control Unit (SCU)	Indicator of the current flow route
SGB 1 Normal Line Status	Subsea Control Unit (SCU)	The status of SGB1 normal line
SGB 1 Bypass Line Status	Subsea Control Unit (SCU)	The status of SGB1 bypass line
SGB 2 Normal Line Status	Subsea Control Unit (SCU)	The status of SGB2 normal line
SGB 2 Bypass Line Status	Subsea Control Unit (SCU)	The status of SGB2 bypass line
SCU Status	Subsea Control Unit (SCU)	The status of Subsea Control Unit (SCU)
SCM Status	Subsea Control Unit (SCU)	The status of Subsea Control Module (SCM)

Subsea Control Unit (SCU)

Table B.3: Control Actions for Loop SCU − SCM

Control Action	Given To	Description
Distribute Control Actions	Subsea Control Module (SCM)	In case of command from operator, the SCU is responsible to distribute the command to the appropriate local SCM

Table B.4: Feedback for Loop SCU − SCM

Feedback	Received From	Description
Control Command	Operator	Control command from the operator
Sensor Reading	Subsea Control Unit (SCU)	Bulk readings from the sensor is gathered at the SCU to be processed and presented to the operator
SGB equipment status	Subsea Control Unit (SCU)	The status of SGB equipment and process line
SCM Status	Subsea Control Unit (SCU)	The status of Subsea Control Module (SCM)

Subsea Control Module (SCM)

Table B.5: Control Actions for Loop SCM − SGB

Control Action	Given To	Description
Adjust Choke Valve Opening (SGB1 Bypass Line)	SGB Bypass Line	Actuation signal to the choke valve
Adjust Oil Multi Phase Pump Variable Speed (SGB1 Normal Line)	SGB Normal Line	Actuation signal to the oil MP pump speed
Adjust Water Multi Phase Pump Variable Speed (SGB1 Normal Line)	SGB Normal Line	Actuation signal to the water MP pump speed
Open Crossover Valve	Subsea Gate Box Crossover Valve	Actuation signal to open crossover valve
Close Crossover Valve	Subsea Gate Box Crossover Valve	Actuation signal to close crossover valve
Open Normal Line Isolation Valve (XV-003 / XV-005)	Subsea Gate Box 1 / 2 Normal Line	Actuation signal to open normal line isolation valve (XV-003 / XV-005)
Close Normal Line Isolation Valve (XV-003 / XV-005)	Subsea Gate Box 1 / 2 Normal Line	Actuation signal to close normal line isolation valve (XV-003 / XV-005)
Open Bypass Line Isolation Valve (XV-002 / XV-004)	Subsea Gate Box 1 / 2 Bypass Line	Actuation signal to open bypass line isolation valve (XV-002 / XV-004)
Close Bypass Line Isolation Valve (XV-002 / XV-004)	Subsea Gate Box 1 / 2 Bypass Line	Actuation signal to close bypass line isolation valve (XV-002 / XV-004)

Table B.6: Feedback for Loop SCM − SGB

Feedback	Received From	Description
Control Command	Subsea Control Module (SCM)	Control command from the operator
Bypass line hydrocarbon pressure	Subsea Control Unit (SCU)	Pressure condition in the bypass process line
Oil MP Pump Differential Pressure	Subsea Control Unit (SCU)	The differences between outlet and inlet pressure of the Oil MP Pump
Water MP Pump Differential Pressure	Subsea Control Unit (SCU)	The differences between outlet and inlet pressure of the Water MP Pump
Flow Route Indicator	Subsea Control Unit (SCU)	Indicator of the current flow route
SGB 1 Normal Line Status	Subsea Control Unit (SCU)	The status of SGB1 normal line
SGB 1 Bypass Line Status	Subsea Control Unit (SCU)	The status of SGB1 bypass line
SGB 2 Normal Line Status	Subsea Control Unit (SCU)	The status of SGB2 normal line
SGB 2 Bypass Line Status	Subsea Control Unit (SCU)	The status of SGB2 bypass line

Appendix C

Basic STPA Results

STPA Analysis Results

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 001	Operator does not adjust set point of choke valve when the pressure of hydrocarbon in the SGB bypass line is high [H1]	SCE.OPE.001.1A0.001	Operator understand that there is significant change of pressure of hydrocarbon in the SGB bypass line, but does not provide set point adjust-ment of choke valve.	-	Unrefined scenario
		SCE.OPE.001.1A1.002	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.001.1B0.003	Operator believes that there is no change of pressure of hydrocarbon in the SGB bypass line, but it is not.	-	Unrefined scenario
		SCE.OPE.001.1B1.004	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	003	BP line pressure sensor failure
		SCE.OPE.001.1B1.005	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	004	BP line pressure sensor miscalibration
		SCE.OPE.001.1B1.006	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.001.2A0.007	Operator gives command to adjust set point of choke valve, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.001.2B0.008	SCU receives the command to adjust set point of choke valve, but it is not followed.	-	Unrefined scenario
		SCE.OPE.001.2B1.009	The command is not followed due to failure in SCU.	024	SCU failure
UCA. OPE. 002	Operator provides wrong set point of choke valve [H1]	SCE.OPE.002.1A0.010	Operator understands the current pressure status in the SGB bypass line, but provides incorrect set point.	-	Unrefined scenario
		SCE.OPE.002.1A1.011	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.002.1A1.012	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.002.1B0.013	Operator receives wrong information regarding the pressure of hydrocarbon in the SGB bypass line.	-	Unrefined scenario
		SCE.OPE.002.1B1.014	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	003	BP line pressure sensor failure
		SCE.OPE.002.1B1.015	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	004	BP line pressure sensor miscalibration
		SCE.OPE.002.1B1.016	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.002.2A0.017	Operator know the correct setpoint, but unknowingly input incorrect number.	019	Operator mistake
		SCE.OPE.002.2B0.018	Operator provides correct command to adjust set point of choke valve, but SCU proceed with incorrect set point.	027	SCU software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 003	Operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass line [H1]	SCE.OPE.003.1A0.019	Operator understands the current pressure status in the SGB bypass line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.003.1A1.020	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.003.1A1.021	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.003.1B0.022	Operator receives late information regarding the pressure of hydrocarbon in the SGB bypass line.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.003.2A0.023	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.003.2B0.024	SCU delays in the processing of command to adjust set point of choke valve.	026	SCU hardware capability
UCA. OPE. 004	Operator reverts the set point of choke valve before the pressure of hydrocarbon in the SGB bypass line return to normal [H1]	SCE.OPE.004.1A0.025	Operator decided to change the set point before the pressure return to the normal condition.	-	Unrefined scenario
		SCE.OPE.004.1A1.026	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.004.1B0.027	Operator believes that the pressure of hydrocarbon in the SGB bypass line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.004.1B1.028	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	003	BP line pressure sensor failure
		SCE.OPE.004.1B1.029	Incorrect feedback about the actual pressure condition of the system is received due to failure of SCU.	004	BP line pressure sensor miscalibration
		SCE.OPE.004.2A0.030	Operator provides correct command of set point, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.004.2B0.031	Operator provides correct command of set point, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	025	SCU failure & software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 005	Operator does not adjust set point of oil MP pump speed when there is a significant change of pressure differences in the oil MP pump [H1, H2]	SCE.OPE.005.1A0.032	Operator understand that there is significant change of hydrocarbon pressure differences in the SGB normal line, but does not provide set point adjustment of oil MP pump speed.	-	Unrefined scenario
		SCE.OPE.005.1A1.033	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.005.1B0.034	Operator believes that there is significant change of hydrocarbon pressure differences in the SGB normal line, but it is not.	-	Unrefined scenario
		SCE.OPE.005.1B1.035	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.005.1B1.036	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	004	BP line pressure sensor miscalibration
		SCE.OPE.005.1B1.037	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.005.2A0.038	Operator gives command to adjust set point of oil MP pump speed, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.005.2B0.039	SCU receives the command to adjust set point of oil MP pump speed, but it is not followed.	-	Unrefined scenario
		SCE.OPE.005.2B1.040	The command is not followed by SCU.	027	SCU software setting
		SCE.OPE.005.2B1.041	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure
UCA. OPE. 006	Operator provides incorrect set point of oil MP pump speed when the hydrocarbon is flowing in the normal line [H1, H2]	SCE.OPE.006.1A0.042	Operator understands the current pressure differences status in the SGB normal line, but provides incorrect set point.	-	Unrefined scenario
		SCE.OPE.006.1A1.043	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.006.1A1.044	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.006.1B0.045	Operator receives wrong information regarding the pressure differences of hydrocarbon in the SGB normal line.	-	Unrefined scenario
		SCE.OPE.006.1B1.046	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.006.1B1.047	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	014	NR line pressure sensor failure
		SCE.OPE.006.1B1.048	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	015	NR line pressure sensor miscalibration
		SCE.OPE.006.2A0.049	Operator know the correct setpoint, but unknowingly input incorrect number.	019	Operator mistake
		SCE.OPE.006.2B0.050	Operator provides correct command to adjust set point of oil MP pump speed, but SCU proceed with incorrect set point.	027	SCU software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 007	Operator provides incorrect set point of oil MP pump speed when the hydrocarbon is flowing in the bypass line [H3]	SCE.OPE.007.1A0.051	Operator think that the flow is flowing in the normal line, when it is not.	-	Unrefined scenario
		SCE.OPE.007.1A1.052	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.007.1A1.053	Operator cannot clearly differentiate between normal process line and bypass process line.	018	Operator knowledge
		SCE.OPE.007.1B0.054	Operator receives wrong information regarding the current active process line in the SGB.	-	Unrefined scenario
		SCE.OPE.007.1B1.055	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	011	NR line & BP line pressure sensor failure
		SCE.OPE.007.1B1.056	Incorrect feedback about the active process line is received due to wrong HMI setting produced by SCU.	027	SCU software setting
		SCE.OPE.007.2B0.057	Operator provides correct command to adjust set point of oil MP pump speed to the normal process line, but SCU proceed with incorrect process line.	027	SCU software setting
UCA. OPE. 008	Operator adjusts set point of separator inlet valve too late during a change of pressure differences in the oil MP pump [H1, H2]	SCE.OPE.008.1A0.058	Operator understands there is significant change of pressure differences in the SGB normal line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.008.1A1.059	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.008.1A1.060	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.008.1B0.061	Operator receives late information regarding the significant change of pressure differences in the SGB normal line.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.008.2A0.062	Communication delay is present during the command from operator to SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.008.2B0.063	SCU delays in the processing of command to adjust set point of oil MP pump speed.	026	SCU hardware capability

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 009	Operator reverts the set point of separator inlet valve before the differential pressure in the oil MP pump return to previous condition [H1, H2]	SCE.OPE.009.1A0.064	Operator decided to change the set point before there is new change of pressure differences in the SGB normal line.		
		SCE.OPE.009.1A1.065	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.009.1B0.066	Operator believes that there is new change of pressure differences in the SGB normal line, but it is not.	-	Unrefined scenario
		SCE.OPE.009.1B1.067	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.009.1B1.068	Incorrect feedback about the actual pressure condition of the system is received due to failure of SCU to generate correct information.	024	SCU failure
		SCE.OPE.009.2A0.069	Inadequate Control Execution: Operator provides correct command of set point, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.009.2B0.070	Operator provides correct command of set point, but abrupt change in SCU signal returning the process to safe state happened due to failure of SCU.	025	SCU failure & software setting
UCA. OPE. 010	Operator does not adjust set point of water MP pump speed when there is a significant change of pressure differences in the water MP pump [H1, H2]	SCE.OPE.010.1A0.071	Operator understand that there is significant change of hydrocarbon pressure differences in the SGB normal line, but does not provide set point adjustment of water MP pump speed.	-	Unrefined scenario
		SCE.OPE.010.1A1.072	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.010.1B0.073	Operator believes that there is significant change of hydrocarbon pressure differences in the SGB normal line, but it is not.	-	Unrefined scenario
		SCE.OPE.010.1B1.074	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.010.1B1.075	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	015	NR line pressure sensor miscalibration
		SCE.OPE.010.1B1.076	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.010.2A0.077	Operator gives command to adjust set point of water MP pump speed, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.010.2B0.078	SCU receives the command to adjust set point of water MP pump speed, but it is not followed.	-	Unrefined scenario
		SCE.OPE.010.2B1.079	The command is not followed by SCU.	027	SCU software setting
		SCE.OPE.010.2B1.080	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA.OPE.011	Operator provides incorrect set point of water MP pump speed when the hydrocarbon is flowing in the normal line [H1, H2]	SCE.OPE.011.1A0.081	Operator understands the current pressure differences status in the SGB normal line, but provides incorrect set point.	-	Unrefined scenario
		SCE.OPE.011.1A1.082	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.011.1A1.083	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.011.1B0.084	Operator receives wrong information regarding the pressure differences of hydrocarbon in the SGB normal line.	-	Unrefined scenario
		SCE.OPE.011.1B1.085	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.011.1B1.086	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	015	NR line pressure sensor miscalibration
		SCE.OPE.011.1B1.087	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.011.2A0.088	Operator know the correct setpoint, but unknowingly input incorrect number.	019	Operator mistake
		SCE.OPE.011.2B0.089	Operator provides correct command to adjust set point of water MP pump speed, but SCU proceed with incorrect set point.	027	SCU software setting
UCA.OPE.012	Operator provides incorrect set point of water MP pump speed when the hydrocarbon is flowing in the bypass line [H3]	SCE.OPE.012.1A0.090	Operator think that the flow is flowing in the normal line, when it is not.	-	Unrefined scenario
		SCE.OPE.012.1A1.091	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.012.1A1.092	Operator cannot clearly differentiate between normal process line and bypass process line.	018	Operator knowledge
		SCE.OPE.012.1B0.093	Operator receives wrong information regarding the current active process line in the SGB.	-	Unrefined scenario
		SCE.OPE.012.1B1.094	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	011	NR line & BP line pressure sensor failure
		SCE.OPE.012.1B1.095	Incorrect feedback about the active process line is received due to wrong HMI setting produced by SCU.	027	SCU software setting
		SCE.OPE.012.2B0.096	Operator provides correct command to adjust set point of water MP pump speed to the normal process line, but SCU proceed with incorrect process line.	027	SCU software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 013	Operator adjusts set point of separator inlet valve too late during a change of pressure differences in the water MP pump [H1, H2]	SCE.OPE.013.1A0.097	Operator understands there is significant change of pressure differences in the SGB normal line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.013.1A1.098	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.013.1A1.099	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.013.1B0.100	Operator receives late information regarding the significant change of pressure differences in the SGB normal line.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.013.2A0.101	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.013.2B0.102	SCU delays in the processing of command to adjust set point of water MP pump speed.	026	SCU hardware capability
UCA. OPE. 014	Operator reverts the set point of separator inlet valve before the differential pressure in the water MP pump return to previous condition [H1, H2]	SCE.OPE.014.1A0.103	Operator decided to change the set point before there is new change of pressure differences in the SGB normal line.	-	Unrefined scenario
		SCE.OPE.014.1A1.104	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.014.1B0.105	Operator believes that there is new change of pressure differences in the SGB normal line, but it is not.	-	Unrefined scenario
		SCE.OPE.014.1B1.106	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.014.1B1.107	Incorrect feedback about the actual pressure condition of the system is received due to failure of SCU to generate correct information.	024	SCU failure
		SCE.OPE.014.2A0.108	Operator provides correct command of set point, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.014.2B0.109	Operator provides correct command of set point, but abrupt change in SCU signal returning the process to safe state happened due to failure of SCU.	025	SCU failure & software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 015	Operator does not change flow line from SGB1 normal line to SGB1 bypass line when SGB1 normal line is faulty [H1, H2, H4]	SCE.OPE.015.1A0.110	Operator understand that SGB1 normal line is faulty, but does not provide command to change flow line from SGB1 normal line to SGB1 bypass line.	-	Unrefined scenario
		SCE.OPE.015.1A1.111	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.015.1B0.112	Operator believes that SGB1 normal line is normal, but it is not.	-	Unrefined scenario
		SCE.OPE.015.1B1.113	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.015.1B1.114	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	015	NR line pressure sensor miscalibration
		SCE.OPE.015.2A0.115	Operator gives command to change flow line from SGB1 normal line to SGB1 bypass line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.015.2B0.116	SCU receives the command to change flow line from SGB1 normal line to SGB1 bypass line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.015.2B1.117	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure
UCA. OPE. 016	Operator changes flow line from SGB1 normal line to SGB1 bypass line when both SGB 1 normal line and bypass line are normal [H4]	SCE.OPE.016.1A0.118	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.016.1A1.119	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.016.1B0.120	Operator receives wrong information regarding the current process status in the SGB1 normal line.	-	Unrefined scenario
		SCE.OPE.016.1B1.121	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.016.1B1.122	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.016.2B0.123	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB1 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 017	Operator changes flow line from SGB1 normal line to SGB1 bypass line when SGB1 bypass line is faulty [H1, H2, H4]	SCE.OPE.017.1A0.124	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.017.1A1.125	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.017.1A1.126	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.017.1B0.127	Operator receives wrong information regarding the current process status in the SGB1 bypass line.	-	Unrefined scenario
		SCE.OPE.017.1B1.128	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.017.1B1.129	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.017.2B0.130	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB1 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 018	Operator changes flow line from SGB1 normal line to SGB1 bypass line when SGB 1 normal line is faulty, SGB1 bypass line is normal but SGB2 normal line is normal [H4]	SCE.OPE.018.1A0.131	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.018.1A1.132	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.018.1A1.133	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.018.1B0.134	Operator receives wrong information regarding the current process status in the SGB1 normal line and SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.018.1B1.135	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.018.1B1.136	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.018.2B0.137	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB1 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 019	Operator changes flow line from SGB1 normal line to SGB1 bypass line too late during the fault condition of SGB1 normal line and normal condition of SGB1 bypass line [H1, H2, H4]	SCE.OPE.019.1A0.138	Operator understands the current process status in the SGB1 normal line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.019.1A1.139	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.019.1A1.140	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.019.1B0.141	Operator receives late information regarding the process status in the SGB1 normal line.	032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate
		SCE.OPE.019.2A0.142	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.019.2B0.143	SCU delays in the processing of command to change flow line from SGB1 normal line to SGB1 bypass line.	026	SCU hardware capability
UCA. OPE. 020	Operator reverts the flow line change command back to SGB1 normal line before SGB1 normal line condition return to normal [H1, H2, H4]	SCE.OPE.020.1A0.144	Operator decided to change the process line before the target process line return to the normal condition.	-	Unrefined scenario
		SCE.OPE.020.1A1.145	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.020.1B0.146	Operator believes that the SGB1 normal line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.020.1B1.147	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.020.1B1.148	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	024	SCU failure
		SCE.OPE.020.2A0.149	Operator provides correct command to use SGB1 bypass line, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.020.2B0.150	Operator provides correct command to use SGB1 bypass line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	025	SCU failure & software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 021	Operator does not change flow line from SGB1 normal line to SGB2 normal line when SGB1 normal line is faulty [H1, H2, H4]	SCE.OPE.021.1A0.151	Operator understand that SGB1 normal line is faulty, but does not provide command to change flow line from SGB1 normal line to SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.021.1A1.152	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.021.1B0.153	Operator believes that SGB1 normal line is normal, but it is not.	-	Unrefined scenario
		SCE.OPE.021.1B1.154	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.021.1B1.155	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.021.2A0.156	Operator gives command to change flow line from SGB1 normal line to SGB2 normal line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.021.2B0.157	SCU receives the command to change flow line from SGB1 normal line to SGB2 normal line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.021.2B1.158	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure
UCA. OPE. 022	Operator changes flow line from SGB1 normal line to SGB2 normal line when both SGB1 normal line and SGB2 normal line are normal [H4]	SCE.OPE.022.1A0.159	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.022.1A1.160	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.022.1B0.161	Operator receives wrong information regarding the current process status in the SGB1 normal line.	-	Unrefined scenario
		SCE.OPE.022.1B1.162	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.022.1B1.163	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.022.2B0.164	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 023	Operator changes flow line from SGB1 normal line to SGB2 normal line when SGB2 normal line is faulty [H1, H2, H4]	SCE.OPE.023.1A0.165	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.023.1A1.166	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.023.1A1.167	Operator has too many process to be considered and mistakes one process to another.	042	Working condition
		SCE.OPE.023.1B0.168	Operator receives wrong information regarding the current process status in the SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.023.1B1.169	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.023.1B1.170	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.023.2B0.171	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 024	Operator changes flow line from SGB1 normal line to SGB2 normal line when the current active process line is in either SGB1 bypass line or SGB2 bypass line [H4]	SCE.OPE.024.1A0.172	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.024.1A1.173	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.024.1B0.174	Operator receives wrong information regarding the current process status in the SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.024.1B1.175	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.024.1B1.176	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.024.2B0.177	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 025	Operator changes flow line from SGB1 normal line to SGB2 normal line too late during the fault condition of SGB1 normal line and normal condition of SGB2 normal line [H1, H2, H4]	SCE.OPE.025.1A0.178	Operator understands the current process status in the SGB1 normal line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.025.1A1.179	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.025.1A1.180	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.025.1B0.181	Operator receives late information regarding the process status in the SGB1 normal line.	032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate
		SCE.OPE.025.2A0.182	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.025.2B0.183	SCU delays in the processing of command to change flow line from SGB1 normal line to SGB2 normal line.	026	SCU hardware capability

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 026	Operator reverts the flow line change command back to SGB1 normal line before SGB1 normal line condition return to normal [H1, H2, H4]	SCE.OPE.026.1A0.184	Operator decided to change the process line before the target process line return to the normal condition.	-	Unrefined scenario
		SCE.OPE.026.1A1.185	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.026.1B0.186	Operator believes that the SGB1 normal line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.026.1B1.187	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.026.1B1.188	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	027	SCU software setting
		SCE.OPE.026.2A0.189	Operator provides correct command to use SGB2 normal line, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.026.2B0.190	Operator provides correct command to use SGB2 normal line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	025	SCU failure & software setting
UCA. OPE. 027	Operator does not change flow line from SGB1 normal line to SGB2 bypass line when SGB1 normal line is faulty [H1, H2, H4]	SCE.OPE.027.1A0.191	Operator understand that SGB1 normal line is faulty, but does not provide command to change flow line from SGB1 normal line to SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.027.1A1.192	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.027.1B0.193	Operator believes that SGB1 normal line is normal, but it is not.	-	Unrefined scenario
		SCE.OPE.027.1B1.194	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.027.1B1.195	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.027.2A0.196	Operator gives command to change flow line from SGB1 normal line to SGB2 bypass line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.027.2B0.197	SCU receives the command to change flow line from SGB1 normal line to SGB2 bypass line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.027.2B1.198	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 028	Operator changes flow line from SGB1 normal line to SGB2 bypass line when both SGB1 normal line and SGB2 bypass line are normal [H4]	SCE.OPE.028.1A0.199	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.028.1A1.200	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.028.1B0.201	Operator receives wrong information regarding the current process status in the SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.028.1B1.202	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.028.1B1.203	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.028.2B0.204	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 029	Operator changes flow line from SGB1 normal line to SGB2 bypass when SGB2 bypass line is faulty [H1, H4]	SCE.OPE.029.1A0.205	Operator understands the current process status in the SGB2 bypass line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.029.1A1.206	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.029.1A1.207	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.029.1B0.208	Operator receives wrong information regarding the current process status in the SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.029.1B1.209	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.029.1B1.210	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.029.2B0.211	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 030	Operator changes flow line from SGB1 normal line to SGB2 bypass when SGB1 normal line is faulty and SGB2 bypass line is normal but at least one of either SGB1 bypass line or SGB2 normal line is normal [H4]	SCE.OPE.030.1A0.212	Operator understands the current process status in the SGB1 bypass line or SGB2 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.030.1A1.213	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.030.1A1.214	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.030.1B0.215	Operator receives wrong information regarding the current process status in the SGB1 bypass line or SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.030.1B1.216	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	011	NR line & BP line pressure sensor failure
		SCE.OPE.030.1B1.217	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.030.2B0.218	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 031	Operator changes flow line from SGB1 normal line to SGB2 bypass when the current active process line is in either SGB1 bypass line or SGB2 normal line [H4]	SCE.OPE.031.1A0.219	Operator understands the current process status in the SGB2 bypass line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.031.1A1.220	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.031.1A1.221	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.031.1B0.222	Operator receives wrong information regarding the current process status in the SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.031.1B1.223	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.031.1B1.224	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.031.2B0.225	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 032	Operator changes flow line from SGB1 normal line to SGB2 bypass line too late during the fault condition of SGB1 normal line and normal condition of SGB2 bypass line [H1, H2, H4]	SCE.OPE.032.1A0.226	Operator understands the current process status in the SGB1 normal line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.032.1A1.227	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.032.1A1.228	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.032.1B0.229	Operator receives late information regarding the process status in the SGB1 normal line.	032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate
		SCE.OPE.032.2A0.230	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.032.2B0.231	SCU delays in the processing of command to change flow line from SGB1 normal line to SGB2 bypass line.	026	SCU hardware capability
UCA. OPE. 033	Operator reverts the flow line change command back to SGB1 normal line before SGB1 normal line condition return to normal [H1, H2, H4]	SCE.OPE.033.1A0.232	Operator decided to change the process line before the target process line return to the normal condition.	-	Unrefined scenario
		SCE.OPE.033.1A1.233	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.033.1B0.234	Operator believes that the SGB1 normal line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.033.1B1.235	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.033.1B1.236	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	027	SCU software setting
		SCE.OPE.033.2A0.237	Operator provides correct command to use SGB2 bypass line, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.033.2B0.238	Operator provides correct command to use SGB2 bypass line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	025	SCU failure & software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 034	Operator does not change flow line from SGB1 bypass line to SGB1 normal line when both SGB1 normal line and SGB1 bypass line condition are normal [H4]	SCE.OPE.034.1A0.239	Operator understand that SGB1 normal line is normal, but does not provide command to change flow line from SGB1 bypass line to SGB1 normal line.	-	Unrefined scenario
		SCE.OPE.034.1A1.240	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.034.1B0.241	Operator believes that SGB1 normal line is faulty, but it is not.	-	Unrefined scenario
		SCE.OPE.034.1B1.242	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.034.1B1.243	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.034.2A0.244	Operator gives command to change flow line from SGB1 bypass line to SGB1 normal line, but the command is not received by SCU. \	029	Transmission line HMI - SCU failure
		SCE.OPE.034.2B0.245	SCU receives the command to change flow line from SGB1 bypass line to SGB1 normal line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.034.2B1.246	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure
UCA. OPE. 035	Operator does not change flow line from SGB1 bypass line to SGB1 normal line when SGB1 normal line is faulty [H1, H4]	SCE.OPE.035.1A0.247	Operator understand that SGB1 bypass line is faulty, but does not provide command to change flow line from SGB1 bypass line to SGB1 normal line.	-	Unrefined scenario
		SCE.OPE.035.1A1.248	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.035.1B0.249	Operator believes that SGB1 bypass line is normal, but it is not.	-	Unrefined scenario
		SCE.OPE.035.1B1.250	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.035.1B1.251	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.035.2A0.252	Operator gives command to change flow line from SGB1 bypass line to SGB1 normal line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.035.2B0.253	SCU receives the command to change flow line from SGB1 bypass line to SGB1 normal line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.035.2B1.254	The command is not followed due to failure in SCU to generate correct action.	027	SCU software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 036	Operator changes flow line from SGB1 bypass line to SGB1 normal line when SGB1 normal line condition is faulty [H1, H2, H4]	SCE.OPE.036.1A0.255	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.036.1A1.256	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.036.1A1.257	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.036.1B0.258	Operator receives wrong information regarding the current process status in the SGB1 normal line.	-	Unrefined scenario
		SCE.OPE.036.1B1.259	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.036.1B1.260	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.036.2B0.261	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB1 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 037	Operator changes flow line from SGB1 bypass line to SGB1 normal line too late during the fault condition of SGB1 bypass line and normal condition of SGB1 normal line [H1, H4]	SCE.OPE.037.1A0.262	Operator understands the current process status in the SGB1 bypass line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.037.1A1.263	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.037.1A1.264	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.037.1B0.265	Operator receives late information regarding the process status in the SGB1 bypass line.	032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate
		SCE.OPE.037.2A0.266	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.037.2B0.267	SCU delays in the processing of command to change flow line from SGB1 bypass line to SGB1 normal line.	026	SCU hardware capability

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 038	Operator reverts the flow line change command back to SGB1 bypass line before SGB1 bypass line condition return to normal [H1, H4]	SCE.OPE.038.1A0.268	Operator decided to change the process line before the target process line return to the normal condition.		
		SCE.OPE.038.1A1.269	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.038.1B0.270	Operator believes that the SGB1 bypass line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.038.1B1.271	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.038.1B1.272	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	027	SCU software setting
		SCE.OPE.038.2A0.273	Operator provides correct command to use SGB1 normal line, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.038.2B0.274	Operator provides correct command to use SGB1 normal line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	025	SCU failure & software setting
UCA. OPE. 039	Operator does not change flow line from SGB1 bypass line to SGB2 normal line when SGB2 normal line condition is normal [H4]	SCE.OPE.039.1A0.275	Operator understand that SGB2 normal line is normal, but does not provide command to change flow line from SGB1 bypass line to SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.039.1A1.276	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.039.1B0.277	Operator believes that SGB2 normal line is faulty, but it is not.	-	Unrefined scenario
		SCE.OPE.039.1B1.278	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.039.1B1.279	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.039.2A0.280	Operator gives command to change flow line from SGB1 bypass line to SGB2 normal line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.039.2B0.281	SCU receives the command to change flow line from SGB1 bypass line to SGB2 normal line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.039.2B1.282	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 040	Operator does not change flow line from SGB1 bypass line to SGB2 normal line when SGB1 bypass line is faulty [H1, H4]	SCE.OPE.040.1A0.283	Operator understand that SGB1 bypass line is faulty, but does not provide command to change flow line from SGB1 bypass line to SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.040.1A1.284	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.040.1B0.285	Operator believes that SGB1 bypass line is normal, but it is not.	-	Unrefined scenario
		SCE.OPE.040.1B1.286	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.040.1B1.287	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.040.2A0.288	Operator gives command to change flow line from SGB1 bypass line to SGB2 normal line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.040.2B0.289	SCU receives the command to change flow line from SGB1 bypass line to SGB2 normal line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.040.2B1.290	The command is not followed due to failure in SCU to generate correct action.	027	SCU software setting
UCA. OPE. 041	Operator changes flow line from SGB1 bypass line to SGB2 normal line when SGB1 normal line is normal [H4]	SCE.OPE.041.1A0.291	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.041.1A1.292	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.041.1A1.293	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.041.1B0.294	Operator receives wrong information regarding the current process status in the SGB1 normal line.	-	Unrefined scenario
		SCE.OPE.041.1B1.295	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.041.1B1.296	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.041.2B0.297	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 042	Operator changes flow line from SGB1 bypass line to SGB2 normal line when SGB2 normal line is faulty [H1, H2, H4]	SCE.OPE.042.1A0.298	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.042.1A1.299	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.042.1A1.300	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.042.1B0.301	Operator receives wrong information regarding the current process status in the SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.042.1B1.302	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.042.1B1.303	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.042.2B0.304	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 043	Operator changes flow line from SGB1 bypass line to SGB2 normal line when the current active process line is in either SGB1 normal line or SGB2 bypass line [H4]	SCE.OPE.043.1A0.305	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.043.1A1.306	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.043.1A1.307	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.043.1B0.308	Operator receives wrong information regarding the current process status in the SGB2 normal line.	-	Unrefined scenario
		SCE.OPE.043.1B1.309	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
		SCE.OPE.043.1B1.310	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.043.2B0.311	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 normal line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 044	Operator changes flow line from SGB1 bypass line to SGB2 normal line too late during the fault condition of SGB1 bypass line and normal condition of SGB2 normal line [H1, H4]	SCE.OPE.044.1A0.312	Operator understands the current process status in the SGB1 bypass line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.044.1A1.313	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.044.1A1.314	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.044.1B0.315	Operator receives late information regarding the process status in the SGB1 bypass line.	032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate
		SCE.OPE.044.2A0.316	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.044.2B0.317	SCU delays in the processing of command to change flow line from SGB1 bypass line to SGB2 normal line.	026	SCU hardware capability
UCA. OPE. 045	Operator reverts the flow line change command back to SGB1 bypass line before SGB1 bypass line condition return to normal [H1, H2, H4]	SCE.OPE.045.1A0.318	Operator decided to change the process line before the target process line return to the normal condition.	-	Unrefined scenario
		SCE.OPE.045.1A1.319	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.045.1B0.320	Operator believes that the SGB1 bypass line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.045.1B1.321	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.045.1B1.322	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	027	SCU software setting
		SCE.OPE.045.2A0.323	Operator provides correct command to use SGB2 normal line, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.045.2B0.324	Operator provides correct command to use SGB2 normal line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	024	SCU failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 046	Operator does not change flow line from SGB1 bypass line to SGB2 bypass line when SGB1 bypass line is faulty [H1, H4]	SCE.OPE.046.1A0.325	Operator understand that SGB1 bypass line is faulty, but does not provide command to change flow line from SGB1 bypass line to SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.046.1A1.326	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.046.1B0.327	Operator believes that SGB1 bypass line is normal, but it is not.	-	Unrefined scenario
		SCE.OPE.046.1B1.328	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.046.1B1.329	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.046.2A0.330	Operator gives command to change flow line from SGB1 bypass line to SGB2 bypass line, but the command is not received by SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.046.2B0.331	SCU receives the command to change flow line from SGB1 bypass line to SGB2 bypass line, but it is not followed.	-	Unrefined scenario
		SCE.OPE.046.2B1.332	The command is not followed due to failure in SCU to generate correct action.	024	SCU failure
UCA. OPE. 047	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when SGB1 bypass line is faulty, SGB2 bypass line is normal and at least one of either SGB1 normal line or SGB2 normal line is normal [H4]	SCE.OPE.047.1A0.333	Operator understands the current process status in all SGB process line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.047.1A1.334	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.047.1A1.335	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.047.1B0.336	Operator receives wrong information regarding the current process status in the all SGB process line.	-	Unrefined scenario
		SCE.OPE.047.1B1.337	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	011	NR line & BP line pressure sensor failure
		SCE.OPE.047.1B1.338	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.047.2B0.339	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	029	Transmission line HMI - SCU failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 048	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when both SGB1 bypass line and SGB2 bypass line are normal [H4]	SCE.OPE.048.1A0.340	Operator understands the current process status in SGB2 bypass line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.048.1A1.341	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.048.1A1.342	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.048.1B0.343	Operator receives wrong information regarding the current process status in the SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.048.1B1.344	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.048.1B1.345	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.048.2B0.346	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 049	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when SGB2 bypass line is faulty [H1, H4]	SCE.OPE.049.1A0.347	Operator understands the current process status in SGB2 bypass line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.049.1A1.348	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.049.1A1.349	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.049.1B0.350	Operator receives wrong information regarding the current process status in the SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.049.1B1.351	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.049.1B1.352	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.049.2B0.353	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 050	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when the current active process line is in either SGB1 normal line or SGB2 normal line [H4]	SCE.OPE.050.1A0.354	Operator understands the current process status in SGB2 bypass line, but made incorrect decisions.	-	Unrefined scenario
		SCE.OPE.050.1A1.355	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.050.1A1.356	Operator has too many process to be considered and mistakes one process to another.	019	Operator mistake
		SCE.OPE.050.1B0.357	Operator receives wrong information regarding the current process status in the SGB2 bypass line.	-	Unrefined scenario
		SCE.OPE.050.1B1.358	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.050.1B1.359	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	027	SCU software setting
		SCE.OPE.050.2B0.360	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA. OPE. 051	Operator changes flow line from SGB1 bypass line to SGB2 bypass line too late during the fault condition of SGB1 bypass line and normal condition of SGB2 bypass line [H1, H4]	SCE.OPE.051.1A0.361	Operator understands the current process status in the SGB1 bypass line, but takes long time to provide actions.	-	Unrefined scenario
		SCE.OPE.051.1A1.362	Operator is under pressure due to too many responsibilities and process to be considered.	042	Working condition
		SCE.OPE.051.1A1.363	A long procedure need to be taken before giving decision.	028	Task procedure
		SCE.OPE.051.1B0.364	Operator receives late information regarding the process status in the SGB1 bypass line.	032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate
		SCE.OPE.051.2A0.365	Communication delay is present during the command from operator to SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.OPE.051.2B0.366	SCU delays in the processing of command to change flow line from SGB1 bypass line to SGB2 bypass line.	026	SCU hardware capability

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. OPE. 052	Operator reverts the flow line change command back to SGB1 bypass line before SGB1 bypass line condition return to normal [H1, H2, H4]	SCE.OPE.052.1A0.367	Operator decided to change the process line before the target process line return to the normal condition.	-	Unrefined scenario
		SCE.OPE.052.1A1.368	Lack of understanding to the appropriate respond when facing the situation.	018	Operator knowledge
		SCE.OPE.052.1B0.369	Operator believes that the SGB1 bypass line has returned to normal, but it is not.	-	Unrefined scenario
		SCE.OPE.052.1B1.370	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	003	BP line pressure sensor failure
		SCE.OPE.052.1B1.371	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	027	SCU software setting
		SCE.OPE.052.2A0.372	Operator provides correct command to use SGB2 bypass line, but abrupt change happened due to loss of communication between operator HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.OPE.052.2B0.373	Operator provides correct command to use SGB2 bypass line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	025	SCU failure & software setting
UCA. SCU.0 53	SCU does not distribute control actions when there is a command to distribute control [H1, H2, H3, H4]	SCE.SCU.053.1A0.374	SCU receives command from the operator, but it does not distribute the control action to SCM.	-	Unrefined scenario
		SCE.SCU.053.1A1.375	SCU does not process the command due to missing/wrong logic in the program.	027	SCU software setting
		SCE.SCU.053.1B0.376	SCU does not receive the command from the operator to distribute control.	-	Unrefined scenario
		SCE.SCU.053.1B1.377	SCU does not receive command from the operator due to loss of communication between HMI and SCU.	029	Transmission line HMI - SCU failure
		SCE.SCU.053.2A0.378	SCU distributes control actions, but the command is not received by SCM.	036	Transmission line SCU - SCM failure
		SCE.SCU.053.2B0.379	SCU distributes control action to SCM, but it is not followed due to failure in SCM to generate correct action.	020	SCM failure
UCA. SCU.0 54	SCU distribute wrong control actions to SCM when there is command for control action distribution [H1, H2, H3, H4]	SCE.SCU.054.1A0.380	SCU receives correct command, but generate a wrong signal due to wrong logic in the software.	027	SCU software setting
		SCE.SCU.054.1B0.381	SCU receives wrong command from the operator.	019	Operator mistake
		SCE.SCU.054.2A0.382	SCU distributes control actions to the correct SCM but is not received due to loss of communication line between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCU.054.2B0.383	SCU distributes correct control actions to SCM, but SCM proceeds with incorrect actions.	023	SCM software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA.SCU.055	SCU distribute control actions to the wrong SCM when there is command for control action distribution [H1, H2, H3, H4]	SCE.SCU.055.1A0.384	SCU receives command to distribute control actions, but distribute it to the wrong SCM due to wrong logic in the software.	027	SCU software setting
		SCE.SCU.055.1B0.385	SCU receives wrong command from the operator.	019	Operator mistake
		SCE.SCU.055.2A0.386	SCU distributes control actions correctly, but received by the wrong SCM.	027	SCU software setting
UCA.SCU.056	SCU distribute control actions without any command from the operator [H1, H2, H3, H4]	SCE.SCU.056.1A0.387	SCU believes that there is command, but it is not.	-	Unrefined scenario
		SCE.SCU.056.1A1.388	Wrong logic in the program initiate signal without any command.	027	SCU software setting
		SCE.SCU.056.1B0.389	SCU receives spurious trip signal to distribute control command due to noise in the communication line.	030	Transmission line HMI - SCU noise
UCA.SCU.057	SCU distribute control actions too late during demand of distribute control actions [H1, H2, H3, H4]	SCE.SCU.057.1A0.390	SCU understands that there is command from the operator, but takes long time to distribute signal.	-	Unrefined scenario
		SCE.SCU.057.1A1.391	High load in the process memory due to too many process to be considered.	026	SCU hardware capability
		SCE.SCU.057.1B0.392	SCU receives late information regarding the command from the operator due to communication delay between operator and SCU.	031	Transmission line HMI - SCU transfer rate
		SCE.SCU.057.2A0.393	Communication delay is present during the command from SCU to SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCU.057.2B0.394	SCM delays in the processing of command by SCU.	022	SCM hardware capability
UCA.SCU.058	SCU stop distributing control actions before the command to distribute control actions is stopped/changed [H1, H2, H3, H4]	SCE.SCU.058.1B0.395	SCU believes that the command to distribute control actions is stopped, but it is not.	-	Unrefined scenario
		SCE.SCU.058.1B1.396	SCU receives spurious trip signal to stop distribute control command due to noise in the communication line.	030	Transmission line HMI - SCU noise
		SCE.SCU.058.2A0.397	SCU distributes control actions correctly, but abrupt change happened due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCU.058.2B0.398	SCU provides correct command of set point, but abrupt change in SCM signal returning the process to safe state happened due to failure of SCM.	021	SCM failure & software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 059	SCM does not modify choke valve opening when there is SCU command to modify choke valve opening [H1]	SCE.SCM.059.1A0.399	SCM receives command from SCU, but it does not modify the choke valve opening.	-	Unrefined scenario
		SCE.SCM.059.1A1.400	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.059.1B0.401	SCM does not receive the command from SCU to modify choke valve opening.	-	Unrefined scenario
		SCE.SCM.059.1B1.402	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.059.2A0.403	SCM modifies choke valve opening, but the command is not received by the choke valve (on SGB bypass line).	033	Transmission line SCM - SGB failure
		SCE.SCM.059.2B0.404	SCM generates signal to modify choke valve opening correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.059.2B1.405	Failure happened in the choke valve.	005	Choke valve failure
		SCE.SCM.059.2B1.406	Insufficient pressure to actuate the choke valve in the hydraulic accumulator.	009	Insufficient hydraulic pressure
UCA. SCM. 060	SCM modifies choke valve opening with incorrect signal [H1]	SCE.SCM.060.1A0.407	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.060.1B0.408	SCM receives wrong command from SCU.	027	SCU software setting
		SCE.SCM.060.2A0.409	SCM modifies choke valve opening correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
UCA. SCM. 061	SCM modifies choke valve opening too late during SCU command to modify choke valve opening [H1]	SCE.SCM.061.1A0.410	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.061.1A1.411	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.061.1B0.412	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.061.2A0.413	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.061.2B0.414	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.061.2B1.415	Insufficient pressure to actuate the choke valve.	009	Insufficient hydraulic pressure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 062	SCM reverts choke valve opening before SCU command to modify choke valve opening is stopped [H1]	SCE.SCM.062.1B0.416	SCM believes that the command to modify choke valve opening is stopped, but it is not.	-	Unrefined scenario
		SCE.SCM.062.1B1.417	SCM receives spurious trip signal to modify choke valve opening due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.062.2A0.418	SCM generates correct command to modify choke valve opening, but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.062.2B0.419	SCM provides correct signal to modify choke valve opening, but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	006	Choke valve failure & setting
UCA. SCM. 063	SCM does not modify oil MP pump variable speed when there is SCU command to modify oil MP pump variable speed [H1, H2]	SCE.SCM.063.1A0.420	SCM receives command from SCU, but it does not modify the oil MP pump variable speed.	-	Unrefined scenario
		SCE.SCM.063.1A1.421	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.063.1B0.422	SCM does not receive the command from SCU to modify oil MP pump variable speed.	-	Unrefined scenario
		SCE.SCM.063.1B1.423	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.063.2A0.424	SCM modifies oil MP pump variable speed, but the command is not received by the oil MP pump (on SGB normal line).	033	Transmission line SCM - SGB failure
		SCE.SCM.063.2B0.425	SCM generates signal to modify choke valve opening correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.063.2B1.426	Failure happened in the water MP pump variable speed drive.	017	Oil MP pump vsd failure
		SCE.SCM.063.2B1.427	Failure happened in the oil MP pump.	016	Oil MP pump failure
UCA. SCM. 064	SCM modifies oil MP pump variable speed with incorrect signal when the flow is flowing in the normal line [H1, H2]	SCE.SCM.064.1A0.428	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.064.1B0.429	SCM receives wrong command from SCU.	027	SCU software setting
		SCE.SCM.064.2A0.430	SCM modifies oil MP pump variable speed opening correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
UCA. SCM. 065	SCM modifies oil MP pump variable speed with incorrect signal when the flow is flowing in the bypass line [H3]	SCE.SCM.065.1A0.431	SCM think that the flow is flowing in the normal line, when it is not.	014	NR line pressure sensor failure
		SCE.SCM.065.1B0.432	SCM receives wrong information regarding the current active process line in the SGB.	-	Unrefined scenario
		SCE.SCM.065.1B1.433	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 066	SCM modifies oil MP pump variable speed too late during SCU command to modify oil MP pump variable speed [H1, H2]	SCE.SCM.066.1A0.434	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.066.1A1.435	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.066.1B0.436	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.066.2A0.437	Communication delay is present during the command from SCM to the variable speed drive.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.066.2B0.438	Variable speed drive delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.066.2B1.439	insufficient power to actuate the variable speed drive.	010	Insufficient power supply
UCA. SCM. 067	SCM reverts oil MP pump variable speed before SCU command to modify oil MP pump variable speed is stopped [H1, H2]	SCE.SCM.067.1B0.440	SCM believes that the command to modify oil MP pump variable speed is stopped, but it is not.	-	Unrefined scenario
		SCE.SCM.067.1B1.441	SCM receives spurious trip signal to modify oil MP pump variable speed due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.067.2A0.442	SCM generates correct command to modify oil MP pump speed, but abrupt change happened due to loss of communication between SCM and the variable speed drive.	033	Transmission line SCM - SGB failure
		SCE.SCM.067.2B0.443	SCM provides correct signal to modify oil MP pump variable speed, but abrupt change in variable speed drive signal returning the process to safe state happened due to failure of variable speed drive.	039	VSD failure & VSD setting
UCA. SCM. 068	SCM does not modify water MP pump variable speed when there is SCU command to modify water MP pump variable speed [H1, H2]	SCE.SCM.068.1A0.444	SCM receives command from SCU, but it does not modify the water MP pump variable speed.	-	Unrefined scenario
		SCE.SCM.068.1A1.445	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.068.1B0.446	SCM does not receive the command from SCU to modify water MP pump variable speed.	-	Unrefined scenario
		SCE.SCM.068.1B1.447	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.068.2A0.448	SCM modifies water MP pump variable speed, but the command is not received by the water MP pump (on SGB normal line).	033	Transmission line SCM - SGB failure
		SCE.SCM.068.2B0.449	SCM generates signal to modify choke valve opening correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.068.2B1.450	Failure happened in the water MP pump variable speed drive.	041	Water MP pump vsd failure
		SCE.SCM.068.2B1.451	Failure happened in the water MP pump.	040	Water MP pump failure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 069	SCM modifies water MP pump variable speed with incorrect signal when the flow is flowing in the normal line [H1, H2]	SCE.SCM.069.1A0.452	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.069.1B0.453	SCM receives wrong command from SCU.	027	SCU software setting
		SCE.SCM.069.2A0.454	SCM modifies water MP pump variable speed opening correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
UCA. SCM. 070	SCM modifies water MP pump variable speed with incorrect signal when the flow is flowing in the bypass line [H3]	SCE.SCM.070.1A0.455	SCM think that the flow is flowing in the normal line, when it is not.	014	NR line pressure sensor failure
		SCE.SCM.070.1B0.456	SCM receives wrong information regarding the current active process line in the SGB.	-	Unrefined scenario
		SCE.SCM.070.1B1.457	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	014	NR line pressure sensor failure
UCA. SCM. 071	SCM modifies water MP pump variable speed too late during SCU command to modify water MP pump variable speed [H1, H2]	SCE.SCM.071.1A0.458	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.071.1A1.459	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.071.1B0.460	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.071.2A0.461	Communication delay is present during the command from SCM to the variable speed drive.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.071.2B0.462	Variable speed drive delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.071.2B1.463	Insufficient power to actuate the variable speed drive.	010	Insufficient power supply
UCA. SCM. 072	SCM reverts water MP pump variable speed before SCU command to modify water MP pump variable speed is stopped [H1, H2]	SCE.SCM.072.1B0.464	SCM believes that the command to modify water MP pump variable speed is stopped, but it is not.	-	Unrefined scenario
		SCE.SCM.072.1B1.465	SCM receives spurious trip signal to modify water MP pump variable speed due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.072.2A0.466	SCM generates correct command to modify water MP pump speed, but abrupt change happened due to loss of communication between SCM and the variable speed drive.	033	Transmission line SCM - SGB failure
		SCE.SCM.072.2B0.467	SCM provides correct signal to modify water MP pump variable speed, but abrupt change in variable speed drive signal returning the process to safe state happened due to failure of variable speed drive.	039	VSD failure & VSD setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 073	SCM does not open crossover valve when there is SCU command to open crossover valve [H1, H2, H4]	SCE.SCM.073.1A0.468	SCM receives command from SCU, but it does not open the crossover valve.	-	Unrefined scenario
		SCE.SCM.073.1A1.469	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.073.1B0.470	SCM does not receive the command from SCU to open crossover valve.	-	Unrefined scenario
		SCE.SCM.073.1B1.471	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.073.2A0.472	SCM provides signal to open crossover valve correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.073.2B0.473	SCM generates signal to open crossover valve correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.073.2B1.474	Failure happened in the crossover valve.	007	Crossover valve failure
		SCE.SCM.073.2B1.475	Insufficient pressure to actuate the crossover valve in the hydraulic accumulator.	009	Insufficient hydraulic pressure
UCA. SCM. 074	SCM gives incorrect signal during SCU command to open crossover valve [H1, H2, H4]	SCE.SCM.074.1A0.476	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.074.1B0.477	SCM receives wrong command from SCU.	027	SCU software setting
UCA. SCM. 075	SCM opens crossover valve too late during SCU command to open crossover valve [H1, H2, H4]	SCE.SCM.075.1A0.478	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.075.1A1.479	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.075.1B0.480	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.075.2A0.481	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.075.2B0.482	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.075.2B1.483	Insufficient pressure to actuate the crossover valve.	009	Insufficient hydraulic pressure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 076	SCM closes crossover valve before SCU command to open crossover valve is stopped [H1, H2, H4]	SCE.SCM.076.1B0.484	SCM believes that the command to open crossover valve is changed, but it is not.	-	Unrefined scenario
		SCE.SCM.076.1B1.485	SCM receives spurious trip signal to close crossover valve due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.076.2A0.486	SCM generates correct command to open crossover valve, but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.076.2B0.487	SCM provides correct signal to open crossover valve, but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	008	Crossover valve failure & setting
UCA. SCM. 077	SCM does not close crossover valve when there is SCU command to close crossover valve [H4]	SCE.SCM.077.1A0.488	SCM receives command from SCU, but it does not close the crossover valve.	-	Unrefined scenario
		SCE.SCM.077.1A1.489	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.077.1B0.490	SCM does not receive the command from SCU to close crossover valve.	-	Unrefined scenario
		SCE.SCM.077.1B1.491	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.077.2A0.492	SCM provides signal to close crossover valve correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.077.2B0.493	SCM generates signal to close crossover valve correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.077.2B1.494	Failure happened in the crossover valve.	007	Crossover valve failure
		SCE.SCM.077.2B1.495	Insufficient pressure to actuate the crossover valve in the hydraulic accumulator.	009	Insufficient hydraulic pressure
UCA. SCM. 078	SCM gives incorrect signal during SCU command to close crossover valve [H4]	SCE.SCM.078.1A0.496	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.078.1B0.497	SCM receives wrong command from SCU.	-	Unrefined scenario
UCA. SCM. 079	SCM closes crossover valve without SCU command to close crossover valve [H1, H2, H4]	SCE.SCM.079.1B1.498	SCM receives spurious trip signal to close crossover valve due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.079.2B0.499	Actuator receives spurious trip signal to close crossover valve due to noise in the communication line.	-	Unrefined scenario

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 080	SCM closes crossover valve too late during SCU command to close crossover valve [H4]	SCE.SCM.080.1A0.500	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.080.1A1.501	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.080.1B0.502	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.080.2A0.503	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.080.2B0.504	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.080.2B1.505	Insufficient pressure to actuate the crossover valve.	009	Insufficient hydraulic pressure
UCA. SCM. 081	SCM opens crossover valve before SCU command to close crossover valve is stopped [H4]	SCE.SCM.081.1B0.506	SCM believes that the command to close crossover valve is changed, but it is not.	-	Unrefined scenario
		SCE.SCM.081.1B1.507	SCM receives spurious trip signal to close crossover valve due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.081.2A0.508	SCM generates correct command to close crossover valve, but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.081.2B0.509	SCM provides correct signal to open crossover valve, but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	008	Crossover valve failure & setting
UCA. SCM. 082	SCM does not open normal line isolation valve (XV-003 / XV-005) when there is SCU command to open normal line isolation valve (XV-003 / XV-005) [H1, H2, H4]	SCE.SCM.082.1A0.510	SCM receives command from SCU, but it does not open the normal line isolation valve (XV-003 / XV-005)	-	Unrefined scenario
		SCE.SCM.082.1A1.511	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.082.1B0.512	SCM does not receive the command from SCU to open normal line isolation valve (XV-003 / XV-005).	-	Unrefined scenario
		SCE.SCM.082.1B1.513	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.082.2A0.514	SCM provides signal to open normal line isolation valve (XV-003 / XV-005) correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.082.2B0.515	SCM generates signal to open normal line isolation valve (XV-003 / XV-005) correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.082.2B1.516	Failure happened in the normal line isolation valve (XV-003 / XV-005).	012	NR line isolation valve (XV-003 / XV-005) failure
		SCE.SCM.082.2B1.517	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005) in the hydraulic accumulator.	009	Insufficient hydraulic pressure
UCA. SCM. 083	SCM gives incorrect signal during SCU command to open normal line isolation valve (XV-003 / XV-005) [H1, H2, H4]	SCE.SCM.083.1A0.518	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.083.1B0.519	SCM receives wrong command from SCU.	027	SCU software setting

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 084	SCM opens normal line isolation valve (XV-003 / XV-005) too late during SCU command to open normal line isolation valve (XV-003 / XV-005) [H1, H2, H4]	SCE.SCM.084.1A0.520	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.084.1A1.521	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.084.1B0.522	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.084.2A0.523	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.084.2B0.524	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.084.2B1.525	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005).	009	Insufficient hydraulic pressure
UCA. SCM. 085	SCM closes normal line isolation valve (XV-003 / XV-005) before SCU command to open normal line isolation valve (XV-003 / XV-005) is stopped [H1, H2, H4]	SCE.SCM.085.1B0.526	SCM believes that the command to open normal line isolation valve (XV-003 / XV-005) is changed, but it is not.	-	Unrefined scenario
		SCE.SCM.085.1B1.527	SCM receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.085.2A0.528	SCM generates correct command to open normal line isolation valve (XV-003 / XV-005), but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.085.2B0.529	SCM provides correct signal to open normal line isolation valve (XV-003 / XV-005), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	013	NR line isolation valve (XV-003 / XV-005) failure & setting
UCA. SCM. 086	SCM does not close normal line isolation valve (XV-003 / XV-005) when there is SCU command to close normal line isolation valve (XV-003 / XV-005) [H4]	SCE.SCM.086.1A0.530	SCM receives command from SCU, but it does not close the normal line isolation valve (XV-003 / XV-005).	-	Unrefined scenario
		SCE.SCM.086.1A1.531	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.086.1B0.532	SCM does not receive the command from SCU to close normal line isolation valve (XV-003 / XV-005).	-	Unrefined scenario
		SCE.SCM.086.1B1.533	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.086.2A0.534	SCM provides signal to close normal line isolation valve (XV-003 / XV-005) correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.086.2B0.535	SCM generates signal to close normal line isolation valve (XV-003 / XV-005) correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.086.2B1.536	Failure happened in the normal line isolation valve (XV-003 / XV-005).	012	NR line isolation valve (XV-003 / XV-005) failure
		SCE.SCM.086.2B1.537	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005) in the hydraulic accumulator.	009	Insufficient hydraulic pressure
UCA. SCM. 087	SCM gives incorrect signal during SCU command to close normal line isolation valve (XV-003 / XV-005) [H4]	SCE.SCM.087.1A0.538	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.087.1B0.539	SCM receives wrong command from SCU.	-	Unrefined scenario

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 088	SCM closes normal line isolation valve (XV-003 / XV-005) without SCU command to close normal line isolation valve (XV-003 / XV-005) [H1, H2, H4]	SCE.SCM.088.1B1.540	SCM receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.088.2B0.541	Actuator receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	034	Transmission line SCM - SGB noise
UCA. SCM. 089	SCM closes normal line isolation valve (XV-003 / XV-005) too late during SCU command to close normal line isolation valve (XV-003 / XV-005) [H4]	SCE.SCM.089.1A0.542	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.089.1A1.543	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.089.1B0.544	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.089.2A0.545	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.089.2B0.546	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.089.2B1.547	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005).	009	Insufficient hydraulic pressure
UCA. SCM. 090	SCM opens normal line isolation valve (XV-003 / XV-005) before SCU command to close normal line isolation valve (XV-003 / XV-005) is stopped [H4]	SCE.SCM.090.1B0.548	SCM believes that the command to close normal line isolation valve (XV-003 / XV-005) is changed, but it is not.	-	Unrefined scenario
		SCE.SCM.090.1B1.549	SCM receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.090.2A0.550	SCM generates correct command to close normal line isolation valve (XV-003 / XV-005), but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.090.2B0.551	SCM provides correct signal to open normal line isolation valve (XV-003 / XV-005), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	013	NR line isolation valve (XV-003 / XV-005) failure & setting
UCA. SCM. 091	SCM does not open bypass line isolation valve (XV-002 / XV-004) when there is SCU command to open bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	SCE.SCM.091.1A0.552	SCM receives command from SCU, but it does not open the bypass line isolation valve (XV-002 / XV-004).	-	Unrefined scenario
		SCE.SCM.091.1A1.553	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.091.1B0.554	SCM does not receive the command from SCU to open bypass line isolation valve (XV-002 / XV-004).	-	Unrefined scenario
		SCE.SCM.091.1B1.555	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.091.2A0.556	SCM provides signal to open bypass line isolation valve (XV-002 / XV-004) correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.091.2B0.557	SCM generates signal to open bypass line isolation valve (XV-002 / XV-004) correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.091.2B1.558	Failure happened in the bypass line isolation valve (XV-002 / XV-004).	001	BP line isolation valve (XV-002 / XV-004) failure
		SCE.SCM.091.2B1.559	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004) in the hydraulic accumulator.	009	Insufficient hydraulic pressure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 092	SCM gives incorrect signal during SCU command to open bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	SCE.SCM.092.1A0.560	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.092.1B0.561	SCM receives wrong command from SCU.	027	SCU software setting
UCA. SCM. 093	SCM opens bypass line isolation valve (XV-002 / XV-004) too late during SCU command to open bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	SCE.SCM.093.1A0.562	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.093.1A1.563	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.093.1B0.564	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.093.2A0.565	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.093.2B0.566	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.093.2B1.567	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004).	009	Insufficient hydraulic pressure
UCA. SCM. 094	SCM closes bypass line isolation valve (XV-002 / XV-004) before SCU command to open bypass line isolation valve (XV-002 / XV-004) is stopped [H1, H2, H4]	SCE.SCM.094.1B0.568	SCM believes that the command to open bypass line isolation valve (XV-002 / XV-004) is changed, but it is not.	-	Unrefined scenario
		SCE.SCM.094.1B1.569	SCM receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.094.2A0.570	SCM generates correct command to open bypass line isolation valve (XV-002 / XV-004), but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.094.2B0.571	SCM provides correct signal to open bypass line isolation valve (XV-002 / XV-004), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	002	BP line isolation valve (XV-002 / XV-004) failure & setting
UCA. SCM. 095	SCM does not close bypass line isolation valve (XV-002 / XV-004) when there is SCU command to close bypass line isolation valve (XV-002 / XV-004) [H4]	SCE.SCM.095.1A0.572	SCM receives command from SCU, but it does not close the bypass line isolation valve (XV-002 / XV-004).	-	Unrefined scenario
		SCE.SCM.095.1A1.573	SCM does not process the command due to missing/wrong logic in the program.	023	SCM software setting
		SCE.SCM.095.1B0.574	SCM does not receive the command from SCU to close bypass line isolation valve (XV-002 / XV-004).	-	Unrefined scenario
		SCE.SCM.095.1B1.575	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	036	Transmission line SCU - SCM failure
		SCE.SCM.095.2A0.576	SCM provides signal to close bypass line isolation valve (XV-002 / XV-004) correctly but is not received due to loss of communication line between SCM and actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.095.2B0.577	SCM generates signal to close bypass line isolation valve (XV-002 / XV-004) correctly, but it is not followed.	-	Unrefined scenario
		SCE.SCM.095.2B1.578	Failure happened in the bypass line isolation valve (XV-002 / XV-004).	001	BP line isolation valve (XV-002 / XV-004) failure
		SCE.SCM.095.2B1.579	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004) in the hydraulic accumulator.	009	Insufficient hydraulic pressure

UCA Tag	UCAs	Sce Tag	Scenario	CF Tag	Causal Factor
UCA. SCM. 096	SCM gives incorrect signal during SCU command to close bypass line isolation valve (XV-002 / XV-004) [H4]	SCE.SCM.096.1A0.580	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	023	SCM software setting
		SCE.SCM.096.1B0.581	SCM receives wrong command from SCU.	-	Unrefined scenario
UCA. SCM. 097	SCM closes bypass line isolation valve (XV-002 / XV-004) without SCU command to close bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	SCE.SCM.097.1B1.582	SCM receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.097.2B0.583	Actuator receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	034	Transmission line SCM - SGB noise
UCA. SCM. 098	SCM closes bypass line isolation valve (XV-002 / XV-004) too late during SCU command to close bypass line isolation valve (XV-002 / XV-004) [H4]	SCE.SCM.098.1A0.584	SCM understands that there is command from the operator, but takes long time to generate signal.	-	Unrefined scenario
		SCE.SCM.098.1A1.585	High load in the process memory due to too many process to be considered.	022	SCM hardware capability
		SCE.SCM.098.1B0.586	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	038	Transmission line SCU - SCM transfer rate
		SCE.SCM.098.2A0.587	Communication delay is present during the command from SCM to the actuator.	035	Transmission line SCM - SGB transfer rate
		SCE.SCM.098.2B0.588	Actuator delays in the processing of command by SCM.	-	Unrefined scenario
		SCE.SCM.098.2B1.589	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004).	009	Insufficient hydraulic pressure
UCA. SCM. 099	SCM opens bypass line isolation valve (XV-002 / XV-004) before SCU command to close bypass line isolation valve (XV-002 / XV-004) is stopped [H4]	SCE.SCM.099.1B0.590	SCM believes that the command to close bypass line isolation valve (XV-002 / XV-004) is changed, but it is not.	-	Unrefined scenario
		SCE.SCM.099.1B1.591	SCM receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	037	Transmission line SCU - SCM noise
		SCE.SCM.099.2A0.592	SCM generates correct command to close bypass line isolation valve (XV-002 / XV-004), but abrupt change happened due to loss of communication between SCM and the actuator.	033	Transmission line SCM - SGB failure
		SCE.SCM.099.2B0.593	SCM provides correct signal to open bypass line isolation valve (XV-002 / XV-004), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	002	BP line isolation valve (XV-002 / XV-004) failure & setting

Appendix D

UCA Screening Results

UCA Screening Results

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.OPE.001	Operator does not adjust set point of choke valve when the pressure of hydrocarbon in the SGB bypass line is high [H1]	4	3	3	36	Low	* Automatic control may takeover during emergency * Pressure increases fast	Included
UCA.OPE.002	Operator provides wrong set point of choke valve [H1]	4	3	3	36	Low	* UCA happened during normal/slightly higher pressure condition in the pipeline * Pressure increase / decrease moderately	Included
UCA.OPE.003	Operator adjusts set point of choke valve too late during high pressure of hydrocarbon in the SGB bypass line [H1]	4	4	3	48	Low	* Automatic control does not takeover during emergency * Pressure increases very fast	Included
UCA.OPE.004	Operator reverts the set point of choke valve before the pressure of hydrocarbon in the SGB bypass line return to normal [H1]	4	3	1	12	Low	* Pressure in the process line is still high but already controllable	Screened Out
UCA.OPE.005	Operator does not adjust set point of oil MP pump speed when there is a significant change of pressure differences in the oil MP pump [H1, H2]	4	3	3	36	Medium	* Automatic control may takeover during emergency * Pressure increases fast	Included
UCA.OPE.006	Operator provides incorrect set point of oil MP pump speed when the hydrocarbon is flowing in the normal line [H1, H2]	4	2	3	24	High	* UCA happened during normal/slightly higher pressure condition in the pipeline * Pressure increase / decrease moderately	Included
UCA.OPE.007	Operator provides incorrect set point of oil MP pump speed when the hydrocarbon is flowing in the bypass line [H3]	3	2	1	6	Low	* UCA happened during normal/slightly higher pressure condition in the pipeline * Pressure increase / decrease moderately	Screened Out
UCA.OPE.008	Operator adjusts set point of separator inlet valve too late during a change of pressure differences in the oil MP pump [H1, H2]	4	4	3	48	Medium	* Automatic control does not takeover during emergency * Pressure increases very fast	Included
UCA.OPE.009	Operator reverts the set point of separator inlet valve before the differential pressure in the oil MP pump return to previous condition [H1, H2]	4	3	1	12	Medium	* Pressure in the process line is still high but already controllable	Included
UCA.OPE.010	Operator does not adjust set point of water MP pump speed when there is a significant change of pressure differences in the water MP pump [H1, H2]	4	3	3	36	Medium	* Automatic control may takeover during emergency * Pressure increases fast	Included
UCA.OPE.011	Operator provides incorrect set point of water MP pump speed when the hydrocarbon is flowing in the normal line [H1, H2]	4	2	3	24	High	* UCA happened during normal/slightly higher pressure condition in the pipeline * Pressure increase / decrease moderately	Included
UCA.OPE.012	Operator provides incorrect set point of water MP pump speed when the hydrocarbon is flowing in the bypass line [H3]	3	2	1	6	Low	* UCA happened during normal/slightly higher pressure condition in the pipeline * Pressure increase / decrease moderately	Screened Out
UCA.OPE.013	Operator adjusts set point of separator inlet valve too late during a change of pressure differences in the water MP pump [H1, H2]	4	4	3	48	Medium	* Automatic control does not takeover during emergency * Pressure increases very fast	Included

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.OPE.014	Operator reverts the set point of separator inlet valve before the differential pressure in the water MP pump return to previous condition [H1, H2]	4	3	1	12	Medium	* Pressure in the process line is still high but already controllable	Included
UCA.OPE.015	Operator does not change flow line from SGB1 normal line to SGB1 bypass line when SGB1 normal line is faulty [H1, H2, H4]	4	3	5	60	Low	* Built up pressure is increasing fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.016	Operator changes flow line from SGB1 normal line to SGB1 bypass line when both SGB 1 normal line and bypass line are normal [H4]	2	1	1	2	High	* Both process line is available	Screened Out
UCA.OPE.017	Operator changes flow line from SGB1 normal line to SGB1 bypass line when SGB1 bypass line is faulty [H1, H2, H4]	4	2	1	8	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.018	Operator changes flow line from SGB1 normal line to SGB1 bypass line when SGB 1 normal line is faulty, SGB1 bypass line is normal but SGB2 normal line is normal [H4]	2	2	3	12	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.019	Operator changes flow line from SGB1 normal line to SGB1 bypass line too late during the fault condition of SGB1 normal line and normal condition of SGB1 bypass line [H1, H2, H4]	4	4	5	80	Low	* Built up pressure is increasing very fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.020	Operator reverts the flow line change command back to SGB1 normal line before SGB1 normal line condition return to normal [H1, H2, H4]	4	2	3	24	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Included
UCA.OPE.021	Operator does not change flow line from SGB1 normal line to SGB2 normal line when SGB1 normal line is faulty [H1, H2, H4]	4	3	5	60	Low	* Built up pressure is increasing fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.022	Operator changes flow line from SGB1 normal line to SGB2 normal line when both SGB1 normal line and SGB2 normal line are normal [H4]	2	1	1	2	High	* Both process line is available	Screened Out
UCA.OPE.023	Operator changes flow line from SGB1 normal line to SGB2 normal line when SGB2 normal line is faulty [H1, H2, H4]	4	2	1	8	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.024	Operator changes flow line from SGB1 normal line to SGB2 normal line when the current active process line is in either SGB1 bypass line or SGB2 bypass line [H4]	2	2	1	4	Low	* Two process line is working at the same time * Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.025	Operator changes flow line from SGB1 normal line to SGB2 normal line too late during the fault condition of SGB1 normal line and normal condition of SGB2 normal line [H1, H2, H4]	4	4	5	80	Low	* Built up pressure is increasing very fast * New feature of SGB, experience during unwanted event is limited	Included

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.OPE.026	Operator reverts the flow line change command back to SGB1 normal line before SGB1 normal line condition return to normal [H1, H2, H4]	4	2	3	24	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Included
UCA.OPE.027	Operator does not change flow line from SGB1 normal line to SGB2 bypass line when SGB1 normal line is faulty [H1, H2, H4]	4	3	5	60	Low	* Built up pressure is increasing fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.028	Operator changes flow line from SGB1 normal line to SGB2 bypass line when both SGB1 normal line and SGB2 bypass line are normal [H4]	2	1	1	2	High	* Both process line is available	Screened Out
UCA.OPE.029	Operator changes flow line from SGB1 normal line to SGB2 bypass when SGB2 bypass line is faulty [H1, H4]	4	2	1	8	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.030	Operator changes flow line from SGB1 normal line to SGB2 bypass when SGB1 normal line is faulty and SGB2 bypass line is normal but at least one of either SGB1 bypass line or SGB2 normal line is normal [H4]	2	2	3	12	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.031	Operator changes flow line from SGB1 normal line to SGB2 bypass when the current active process line is in either SGB1 bypass line or SGB2 normal line [H4]	2	2	1	4	Low	* Two process line is working at the same time * Required procedures are able to inform the operator about UCA	Screened Out
UCA.OPE.032	Operator changes flow line from SGB1 normal line to SGB2 bypass line too late during the fault condition of SGB1 normal line and normal condition of SGB2 bypass line [H1, H2, H4]	4	4	5	80	Low	* Built up pressure is increasing very fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.033	Operator reverts the flow line change command back to SGB1 normal line before SGB1 normal line condition return to normal [H1, H2, H4]	4	2	3	24	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Included
UCA.OPE.034	Operator does not change flow line from SGB1 bypass line to SGB1 normal line when both SGB1 normal line and SGB1 bypass line condition are normal [H4]	2	2	1	4	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.035	Operator does not change flow line from SGB1 bypass line to SGB1 normal line when SGB1 bypass line is faulty [H1, H4]	4	3	5	60	Low	* Built up pressure is increasing fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.036	Operator changes flow line from SGB1 bypass line to SGB1 normal line when SGB1 normal line condition is faulty [H1, H2, H4]	4	2	1	8	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.037	Operator changes flow line from SGB1 bypass line to SGB1 normal line too late during the fault condition of SGB1 bypass line and normal condition of SGB1 normal line [H1, H4]	4	4	5	80	Low	* Built up pressure is increasing very fast * New feature of SGB, experience during unwanted event is limited	Included

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.OPE.038	Operator reverts the flow line change command back to SGB1 bypass line before SGB1 bypass line condition return to normal [H1, H4]	4	2	3	24	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Included
UCA.OPE.039	Operator does not change flow line from SGB1 bypass line to SGB2 normal line when SGB2 normal line condition is normal [H4]	2	2	1	4	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.040	Operator does not change flow line from SGB1 bypass line to SGB2 normal line when SGB1 bypass line is faulty [H1, H4]	4	3	5	60	Low	* Built up pressure is increasing fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.041	Operator changes flow line from SGB1 bypass line to SGB2 normal line when SGB1 normal line is normal [H4]	2	2	1	4	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.042	Operator changes flow line from SGB1 bypass line to SGB2 normal line when SGB2 normal line is faulty [H1, H2, H4]	4	2	1	8	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.043	Operator changes flow line from SGB1 bypass line to SGB2 normal line when the current active process line is in either SGB1 normal line or SGB2 bypass line [H4]	2	2	1	4	Low	* Two process line is working at the same time * Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.044	Operator changes flow line from SGB1 bypass line to SGB2 normal line too late during the fault condition of SGB1 bypass line and normal condition of SGB2 normal line [H1, H4]	4	4	5	80	Low	* Built up pressure is increasing very fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.045	Operator reverts the flow line change command back to SGB1 bypass line before SGB1 bypass line condition return to normal [H1, H2, H4]	4	2	3	24	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Included
UCA.OPE.046	Operator does not change flow line from SGB1 bypass line to SGB2 bypass line when SGB1 bypass line is faulty [H1, H4]	4	3	5	60	Low	* Built up pressure is increasing fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.047	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when SGB1 bypass line is faulty, SGB2 bypass line is normal and at least one of either SGB1 normal line or SGB2 normal line is normal [H4]	2	2	1	4	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.048	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when both SGB1 bypass line and SGB2 bypass line are normal [H4]	2	2	1	4	Low	* Inefficient production * Other process lines with higher priority are available	Screened Out
UCA.OPE.049	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when SGB2 bypass line is faulty [H1, H4]	4	2	1	8	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out
UCA.OPE.050	Operator changes flow line from SGB1 bypass line to SGB2 bypass line when the current active process line is in either SGB1 normal line or SGB2 normal line [H4]	2	2	1	4	Low	* Two process line is working at the same time * Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Screened Out

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.OPE.051	Operator changes flow line from SGB1 bypass line to SGB2 bypass line too late during the fault condition of SGB1 bypass line and normal condition of SGB2 bypass line [H1, H4]	4	4	5	80	Low	* Built up pressure is increasing very fast * New feature of SGB, experience during unwanted event is limited	Included
UCA.OPE.052	Operator reverts the flow line change command back to SGB1 bypass line before SGB1 bypass line condition return to normal [H1, H2, H4]	4	2	3	24	Low	* Required procedures are able to inform the operator about UCA * Ample time to prevent implementation of control action	Included
UCA.SCU.053	SCU does not distribute control actions when there is a command to distribute control [H1, H2, H3, H4]	4	4	3	48	High	* Worst-case condition is assumed when the command is related to loss prevention	Included
UCA.SCU.054	SCU distribute wrong control actions to the SCM when there is command for control action distribution [H1, H2, H3, H4]	4	4	3	48	High	* Worst-case condition is assumed when the command is related to loss prevention	Included
UCA.SCU.055	SCU distribute control actions to the wrong SCM when there is command for control action distribution [H1, H2, H3, H4]	4	4	3	48	High	* Worst-case condition is assumed when the command is related to loss prevention	Included
UCA.SCU.056	SCU distribute control actions without any command from the operator [H1, H2, H3, H4]	4	3	3	36	High	* Worst-case condition is assumed when the command may produce an unsafe situation	Included
UCA.SCU.057	SCU distribute control actions too late during demand of distribute control actions [H1, H2, H3, H4]	4	4	3	48	High	* Worst-case condition is assumed when the command is related to loss prevention	Included
UCA.SCU.058	SCU stop distributing control actions before the command to distribute control actions is stopped/changed [H1, H2, H3, H4]	4	3	3	36	High	* Worst-case condition is assumed when the command is related to loss prevention	Included
UCA.SCM.059	SCM does not modify choke valve opening when there is SCU command to modify choke valve opening [H1]	4	3	1	12	Medium	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure increase fast	Included
UCA.SCM.060	SCM modifies choke valve opening with incorrect signal [H1]	4	3	1	12	Medium	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure increase fast	Included
UCA.SCM.061	SCM modifies choke valve opening too late during SCU command to modify choke valve opening [H1]	4	4	3	48	Medium	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure increase fast	Included
UCA.SCM.062	SCM reverts choke valve opening before the SCU command to modify choke valve opening is stopped [H1]	4	2	3	24	Medium	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure has been controlled partially	Included
UCA.SCM.063	SCM does not modify oil MP pump variable speed when there is SCU command to modify oil MP pump variable speed [H1, H2]	4	3	1	12	High	* Worst-case condition is assumed when the command is to actually increase variable speed * Hydrocarbon pressure increase fast	Included
UCA.SCM.064	SCM modifies oil MP pump variable speed with incorrect signal when the flow is flowing in the normal line [H1, H2]	4	3	1	12	High	* Worst-case condition is assumed when the command is to actually increase variable speed * Hydrocarbon pressure increase fast	Included

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.SCM.065	SCM modifies oil MP pump variable speed with incorrect signal when the flow is flowing in the bypass line [H3]	3	2	1	6	Low	* Worst-case condition is assumed when the command is to actually decrease variable speed * Hydrocarbon pressure increase fast	Screened Out
UCA.SCM.066	SCM modifies oil MP pump variable speed too late during SCU command to modify oil MP pump variable speed [H1, H2]	4	4	3	48	High	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure increase fast	Included
UCA.SCM.067	SCM reverts oil MP pump variable speed before the SCU command to modify oil MP pump variable speed is stopped [H1, H2]	4	2	3	24	High	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure has been controlled partially	Included
UCA.SCM.068	SCM does not modify water MP pump variable speed when there is SCU command to modify water MP pump variable speed [H1, H2]	4	3	1	12	HIgh	* Worst-case condition is assumed when the command is to actually increase variable speed * Hydrocarbon pressure increase fast	Included
UCA.SCM.069	SCM modifies water MP pump variable speed with incorrect signal when the flow is flowing in the normal line [H1, H2]	4	3	1	12	High	* Worst-case condition is assumed when the command is to actually increase variable speed * Hydrocarbon pressure increase fast	Included
UCA.SCM.070	SCM modifies water MP pump variable speed with incorrect signal when the flow is flowing in the bypass line [H3]	3	2	1	6	Low	* Worst-case condition is assumed when the command is to actually decrease variable speed * Hydrocarbon pressure increase fast	Screened Out
UCA.SCM.071	SCM modifies water MP pump variable speed too late during SCU command to modify water MP pump variable speed [H1, H2]	4	4	3	48	High	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure increase fast	Included
UCA.SCM.072	SCM reverts water MP pump variable speed before the SCU command to modify water MP pump variable speed is stopped [H1, H2]	4	2	3	24	High	* Worst-case condition is assumed when the command is to actually increase choke valve opening * Hydrocarbon pressure has been controlled partially	Included
UCA.SCM.073	SCM does not open crossover valve when there is SCU command to open crossover valve [H1, H2, H4]	4	3	3	36	Low	* Built up pressure in the blocked process line	Included
UCA.SCM.074	SCM gives incorrect signal during SCU command to open crossover valve [H1, H2, H4]	4	3	3	36	Low	* Built up pressure in the blocked process line	Included
UCA.SCM.075	SCM opens crossover valve too late during SCU command to open crossover valve [H1, H2, H4]	4	4	3	48	Low	* Built up pressure in the blocked process line	Included
UCA.SCM.076	SCM closes crossover valve before the SCU command to open crossover valve is stopped [H1, H2, H4]	4	3	3	36	Low	* Built up pressure in the blocked process line has been controlled partially	Included
UCA.SCM.077	SCM does not close crossover valve when there is SCU command to close crossover valve [H4]	2	2	3	12	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.078	SCM gives incorrect signal during SCU command to close crossover valve [H4]	2	2	3	12	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.079	SCM closes crossover valve without SCU command to close crossover valve [H1, H2, H4]	4	3	3	36	Low	* Built up pressure in the blocked process line	Included
UCA.SCM.080	SCM closes crossover valve too late during SCU command to close crossover valve [H4]	2	3	3	18	Low	* Two process line is working at the same time	Included

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.SCM.081	SCM opens crossover valve before the SCU command to close crossover valve is stopped [H4]	2	2	3	12	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.082	SCM does not open normal line isolation valve (XV-003 / XV-004) when there is SCU command to open normal line isolation valve (XV-003 / XV-004) [H1, H2, H4]	4	3	1	12	Low	* Built up pressure in the blocked process line	Screened Out
UCA.SCM.083	SCM gives incorrect signal during SCU command to open normal line isolation valve (XV-003 / XV-004) [H1, H2, H4]	4	3	1	12	Low	* Built up pressure in the blocked process line	Screened Out
UCA.SCM.084	SCM opens normal line isolation valve (XV-003 / XV-004) too late during SCU command to open normal line isolation valve (XV-003 / XV-004) [H1, H2, H4]	4	4	3	48	Low	* Built up pressure in the blocked process line	Included
UCA.SCM.085	SCM closes normal line isolation valve (XV-003 / XV-004) before the SCU command to open normal line isolation valve (XV-003 / XV-004) is stopped [H1, H2, H4]	4	3	3	36	Low	* Built up pressure in the blocked process line has been controlled partially	Included
UCA.SCM.086	SCM does not close normal line isolation valve (XV-003 / XV-004) when there is SCU command to close normal line isolation valve (XV-003 / XV-004) [H4]	2	2	1	4	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.087	SCM gives incorrect signal during SCU command to close normal line isolation valve (XV-003 / XV-004) [H4]	2	2	1	4	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.088	SCM closes normal line isolation valve (XV-003 / XV-004) without SCU command to close normal line isolation valve (XV-003 / XV-004) [H1, H2, H4]	4	3	1	12	Low	* Built up pressure in the blocked process line has been controlled partially	Screened Out
UCA.SCM.089	SCM closes normal line isolation valve (XV-003 / XV-004) too late during SCU command to close normal line isolation valve (XV-003 / XV-004) [H4]	2	3	3	18	Low	* Two process line is working at the same time	Included
UCA.SCM.090	SCM opens normal line isolation valve (XV-003 / XV-004) before the SCU command to close normal line isolation valve (XV-003 / XV-004) is stopped [H4]	2	2	3	12	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.091	SCM does not open bypass line isolation valve (XV-002 / XV-004) when there is SCU command to open bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	4	3	1	12	Low	* Built up pressure in the blocked process line	Screened Out
UCA.SCM.092	SCM gives incorrect signal during SCU command to open bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	4	3	1	12	Low	* Built up pressure in the blocked process line	Screened Out
UCA.SCM.093	SCM opens bypass line isolation valve (XV-002 / XV-004) too late during SCU command to open bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	4	4	3	48	Low	* Built up pressure in the blocked process line	Included
UCA.SCM.094	SCM closes bypass line isolation valve (XV-002 / XV-004) before the SCU command to open bypass line isolation valve (XV-002 / XV-004) is stopped [H1, H2, H4]	4	3	3	36	Low	* Built up pressure in the blocked process line	Included

UCA Tag	UCAs	Severity	Mitigation	UCA Knowledge	UCAPN	Cond. Event Likelihood	Assumption	Assessment
UCA.SCM.095	SCM does not close bypass line isolation valve (XV-002 / XV-004) when there is SCU command to close bypass line isolation valve (XV-002 / XV-004) [H4]	2	2	1	4	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.096	SCM gives incorrect signal during SCU command to close bypass line isolation valve (XV-002 / XV-004) [H4]	2	2	1	4	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out
UCA.SCM.097	SCM closes bypass line isolation valve (XV-002 / XV-004) without SCU command to close bypass line isolation valve (XV-002 / XV-004) [H1, H2, H4]	4	3	1	12	Low	* Built up pressure in the blocked process line	Screened Out
UCA.SCM.098	SCM closes bypass line isolation valve (XV-002 / XV-004) too late during SCU command to close bypass line isolation valve (XV-002 / XV-004) [H4]	2	3	3	18	Low	* Two process line is working at the same time	Included
UCA.SCM.099	SCM opens bypass line isolation valve (XV-002 / XV-004) before the SCU command to close bypass line isolation valve (XV-002 / XV-004) is stopped [H4]	2	2	3	12	Low	* Two process line is working at the same time * Ample time to prevent UCA	Screened Out

Appendix E

Scenario Ranking Results

Scenario Ranking Results

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.094.2B0.571	SCU does not process the command due to missing/wrong logic in the program.	SCU software setting	027	Systematic	Included	4	4	High	4	3	5	5	320	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.095.1B1.575	SCU receives correct command, but generate a wrong signal due to wrong logic in the software.	SCU software setting	027	Systematic	Included	4	4	High	4	3	5	5	320	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.095.2B1.579	SCU distributes control actions correctly, but received by the wrong SCM.	SCU software setting	027	Systematic	Included	4	4	High	4	3	5	5	320	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.096.1A0.580	SCU receives command to distribute control actions, but distribute it to the wrong SCM due to wrong logic in the software.	SCU software setting	027	Systematic	Included	4	4	High	4	3	5	5	320	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.008.1A1.059	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Medium	3	3	5	5	240	* Probability of event = E-5
SCE.OPE.008.1A1.060	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Medium	3	3	5	5	240	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.013.1A1.098	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Medium	3	3	5	5	240	* Probability of event = E-5
SCE.OPE.013.1A1.099	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Medium	3	3	5	5	240	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.019.2B0.143	SCU delays in the processing of command to change flow line from SGB1 normal line to SGB1 bypass line.	SCU hardware capability	026	Random	Included	4	4	Low	3	5	3	5	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.021.2B1.158	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Included	4	3	Low	4	5	1	5	240	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.025.2B0.183	SCU delays in the processing of command to change flow line from SGB1 normal line to SGB2 normal line.	SCU hardware capability	026	Random	Included	4	4	Low	3	5	3	5	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.027.2B1.198	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Included	4	3	Low	4	5	1	5	240	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.032.2B0.231	SCU delays in the processing of command to change flow line from SGB1 normal line to SGB2 bypass line.	SCU hardware capability	026	Random	Included	4	4	Low	3	5	3	5	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.034.2B1.246	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Included	4	3	Low	4	5	1	5	240	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.037.2B0.267	SCU delays in the processing of command to change flow line from SGB1 bypass line to SGB1 normal line.	SCU hardware capability	026	Random	Included	4	4	Low	3	5	3	5	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.044.2B0.317	SCU delays in the processing of command to change flow line from SGB1 bypass line to SGB2 normal line.	SCU hardware capability	026	Random	Included	4	4	Low	3	5	3	5	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.046.2B1.332	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Included	4	3	Low	4	5	1	5	240	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.051.2B0.366	SCU delays in the processing of command to change flow line from SGB1 bypass line to SGB2 bypass line.	SCU hardware capability	026	Random	Included	4	4	Low	3	5	3	5	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.SCM.059.2B1.405	SCM receives wrong command from SCU.	SCU software setting	027	Systematic	Included	4	3	High	4	1	5	5	240	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.064.1A0.428	SCM receives wrong command from SCU.	SCU software setting	027	Systematic	Included	4	3	High	4	1	5	5	240	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.095.1A1.573	SCU distributes control action to SCM, but it is not followed due to failure in SCM to generate correct action.	SCM failure	020	Random	Included	4	4	High	5	3	3	3	240	* λ = 1.395E-4 (Oreda, 2002, p. 811)
SCE.SCM.097.2B0.583	Wrong logic in the program initiate signal without any command.	SCU software setting	027	Systematic	Included	4	3	High	4	3	5	5	240	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.098.1B0.586	High load in the process memory due to too many process to be considered.	SCU hardware capability	026	Random	Included	4	4	High	5	3	3	3	240	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.008.2A0.062	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	4	Medium	4	3	3	3	192	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.008.2B0.063	SCU delays in the processing of command to adjust set point of oil MP pump speed.	SCU hardware capability	026	Random	Included	4	4	Medium	4	3	3	3	192	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.013.2B0.102	SCU delays in the processing of command to adjust set point of water MP pump speed.	SCU hardware capability	026	Random	Included	4	4	Medium	4	3	3	3	192	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.SCM.061.1A0.410	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	4	4	High	4	3	3	3	192	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCM.066.1A0.434	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	4	4	High	4	3	3	3	192	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCM.094.1B0.568	SCU distributes control actions, but the command is not received by SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	4	High	4	3	3	3	192	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.095.1A0.572	SCU does not receive command from the operator due to loss of communication between HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	4	High	4	3	3	3	192	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.SCM.095.1B0.574	SCU distributes control actions to the correct SCM but is not received due to loss of communication line between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	4	High	4	3	3	3	192	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.095.2B0.577	SCU receives wrong command from the operator.	Operator mistake	019	Random	Included	4	4	High	4	3	3	3	192	* Probability of operator mistake * Assumed as possible to happen
SCE.SCM.096.1B0.581	SCU receives wrong command from the operator.	Operator mistake	019	Random	Included	4	4	High	4	3	3	3	192	* Probability of operator mistake * Assumed as possible to happen
SCE.SCM.098.2B1.589	SCM delays in the processing of command by SCU.	SCM hardware capability	022	Random	Included	4	4	High	4	3	3	3	192	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCU.056.1A0.387	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	4	4	Medium	4	3	3	3	192	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCU.057.2A0.393	Insufficient pressure to actuate the choke valve.	Insufficient hydraulic pressure	009	Random	Included	4	4	Medium	4	3	1	3	192	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.001.1B1.006	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.002.1B1.016	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.002.2B0.018	Operator provides correct command to adjust set point of choke valve, but SCU proceed with incorrect set point.	SCU software setting	027	Systematic	Included	4	3	Low	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.005.1A1.033	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Medium	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.005.1B1.037	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Medium	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.005.2B1.040	The command is not followed by SCU.	SCU software setting	027	Systematic	Included	4	3	Medium	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.009.1A1.065	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Medium	3	1	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.010.1A1.072	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Medium	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.010.1B1.076	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Medium	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.010.2B1.079	The command is not followed by SCU.	SCU software setting	027	Systematic	Included	4	3	Medium	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.014.1A1.104	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Medium	3	1	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.015.2A0.115	Operator gives command to change flow line from SGB1 normal line to SGB1 bypass line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	5	3	5	180	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.021.1B1.155	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	5	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.021.2A0.156	Operator gives command to change flow line from SGB1 normal line to SGB2 normal line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	5	3	5	180	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.027.1B1.195	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	5	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.027.2A0.196	Operator gives command to change flow line from SGB1 normal line to SGB2 bypass line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	5	3	5	180	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.035.1B1.251	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	5	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.035.2A0.252	Operator gives command to change flow line from SGB1 bypass line to SGB1 normal line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	5	3	5	180	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.040.1B1.287	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	5	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.040.2A0.288	Operator gives command to change flow line from SGB1 bypass line to SGB2 normal line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	5	3	5	180	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.040.2B1.290	The command is not followed due to failure in SCU to generate correct action.	SCU software setting	027	Systematic	Included	4	3	Low	3	5	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.046.1B1.329	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	5	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.046.2A0.330	Operator gives command to change flow line from SGB1 bypass line to SGB2 bypass line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	5	3	5	180	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.SCM.059.1A1.400	Failure happened in the water MP pump variable speed drive.	Oil MP pump vsd failure	017	Random	Included	4	3	High	5	1	3	3	180	* λ = 8.795E-5 (Oreda, 2002, p. 334) * Data from general pump topside * T = 10 year
SCE.SCM.059.1B0.401	Failure happened in the oil MP pump.	Oil MP pump failure	016	Random	Included	4	3	High	5	1	3	3	180	* λ = 2.046E-4 (Oreda, 2002, p. 173) * Data from general pump topside * T = 10 year
SCE.SCM.063.2B0.425	Failure happened in the water MP pump variable speed drive.	Water MP pump vsd failure	041	Random	Included	4	3	HIgh	5	1	3	3	180	* λ = 8.795E-5 (Oreda, 2002, p. 334) * Data from general pump topside
SCE.SCM.063.2B1.426	Failure happened in the water MP pump.	Water MP pump failure	040	Random	Included	4	3	HIgh	5	1	3	3	180	* λ = 2.046E-4 (Oreda, 2002, p. 173) * Data from general pump topside * T = 10 year
SCE.SCM.069.2A0.454	SCM receives wrong command from SCU.	SCU software setting	027	Systematic	Included	4	3	Low	3	3	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCU.055.2A0.386	SCM receives wrong command from SCU.	SCU software setting	027	Systematic	Included	4	3	Medium	3	1	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.077.2B1.494	SCM receives wrong command from SCU.	SCU software setting	027	Systematic	Screened Out	4	3	Low	3	1	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.086.2B1.536	SCM receives wrong command from SCU.	SCU software setting	027	Systematic	Screened Out	4	3	Low	3	1	5	5	180	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.003.1A1.020	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	3	5	5	160	* Probability of event = E-5
SCE.OPE.003.1A1.021	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	3	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.006.2B0.050	Operator provides correct command to adjust set point of oil MP pump speed, but SCU proceed with incorrect set point.	SCU software setting	027	Systematic	Included	4	2	High	4	3	5	5	160	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.011.1B1.087	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Included	4	2	High	4	3	5	5	160	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.011.2B0.089	Operator provides correct command to adjust set point of water MP pump speed, but SCU proceed with incorrect set point.	SCU software setting	027	Systematic	Included	4	2	High	4	3	5	5	160	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.019.1A1.139	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	5	5	5	160	* Probability of event = E-5
SCE.OPE.019.1A1.140	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	5	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.025.1A1.179	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	5	5	5	160	* Probability of event = E-5
SCE.OPE.025.1A1.180	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	5	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.032.1A1.227	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	5	5	5	160	* Probability of event = E-5
SCE.OPE.032.1A1.228	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	5	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.037.1A1.263	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	5	5	5	160	* Probability of event = E-5
SCE.OPE.037.1A1.264	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	5	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.044.1A1.313	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	5	5	5	160	* Probability of event = E-5
SCE.OPE.044.1A1.314	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	5	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.051.1A1.362	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Included	4	4	Low	2	3	5	5	160	* Probability of event = E-5
SCE.OPE.051.1A1.363	A long procedure need to be taken before giving decision.	Task procedure	028	Systematic	Included	4	4	Low	2	5	5	5	160	* Systematic error factor, not possible to assign frequency * CF likelihood = Possible
SCE.OPE.001.2B1.009	The command is not followed due to failure in SCU.	SCU failure	024	Random	Included	4	3	Low	4	3	1	3	144	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.003.2B0.024	SCU delays in the processing of command to adjust set point of choke valve.	SCU hardware capability	026	Random	Included	4	4	Low	3	3	3	3	144	* λ = 9.575E-5 (Oreda, 2002, p. 811) * 11/21 Failure due to fail to function on demand, Erratic output & Fail to function while running (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.005.2A0.038	Operator gives command to adjust set point of oil MP pump speed, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Medium	4	3	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.005.2B1.041	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Included	4	3	Medium	4	3	1	3	144	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.009.2A0.069	Inadequate Control Execution: Operator provides correct command of set point, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Medium	4	1	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.009.2B0.070	Operator provides correct command of set point, but abrupt change in SCU signal returning the process to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	3	Medium	4	1	3	3	144	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.OPE.010.2A0.077	Operator gives command to adjust set point of water MP pump speed, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Medium	4	3	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.014.2A0.108	Operator provides correct command of set point, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Medium	4	1	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.014.2B0.109	Operator provides correct command of set point, but abrupt change in SCU signal returning the process to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	3	Medium	4	1	3	3	144	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.SCM.059.2A0.403	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	3	High	4	1	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.061.2B0.414	insufficient power to actuate the variable speed drive.	Insufficient power supply	010	Random	Included	4	4	High	3	3	3	3	144	* λ = 1.016E-6 (Oreda, 2002, p. 811) T = 10 year
SCE.SCM.063.1B0.422	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	3	HIgh	4	1	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.066.2B0.438	Insufficient power to actuate the variable speed drive.	Insufficient power supply	010	Random	Included	4	4	High	3	3	3	3	144	* λ = 1.016E-6 (Oreda, 2002, p. 811) T = 10 year
SCE.SCM.070.1A0.455	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	4	4	Low	3	3	3	3	144	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCM.078.1B0.497	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	4	4	Low	3	3	3	3	144	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCM.087.1B0.539	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	4	4	Low	3	3	3	3	144	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCM.095.2B1.578	SCU distributes correct control actions to SCM, but SCM proceeds with incorrect actions.	SCM software setting	023	Systematic	Included	4	4	High	3	3	3	3	144	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.098.2A0.587	SCU receives spurious trip signal to distribute control command due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Included	4	3	High	4	3	3	3	144	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.099.1B1.591	SCU receives spurious trip signal to stop distribute control command due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Included	4	3	High	4	3	3	3	144	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.SCM.099.2A0.592	SCU distributes control actions correctly, but abrupt change happened due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	3	High	4	3	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.099.2B0.593	SCU provides correct command of set point, but abrupt change in SCM signal returning the process to safe state happened due to failure of SCM.	SCM failure & software setting	021	Random & Systematic	Included	4	3	High	4	3	3	3	144	* λ = 1.395E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 Year
SCE.SCU.053.1B1.377	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	3	Medium	4	1	3	3	144	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCU.054.2A0.382	Failure happened in the choke valve.	Choke valve failure	005	Random	Included	4	3	Medium	4	1	3	3	144	* λ = 2.533E-5 (Oreda, 2002, p. 833) * T = 10 year
SCE.OPE.001.1A1.002	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.002.1A1.011	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.006.1A1.043	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	High	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.010.2B1.080	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Included	4	2	High	5	3	1	3	120	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.011.1A1.082	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	High	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.015.1A1.111	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	5	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.015.1B1.113	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	3	Low	2	5	1	5	120	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.021.1A1.152	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	5	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.021.1B1.154	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	3	Low	2	5	1	5	120	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.027.1A1.192	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	5	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.027.1B1.194	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	3	Low	2	5	1	5	120	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.035.1A1.248	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	5	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.035.1B1.250	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	3	Low	2	5	1	5	120	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.040.1A1.284	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	5	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.040.1B1.286	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	3	Low	2	5	1	5	120	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.046.1A1.326	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	3	Low	2	5	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.046.1B1.328	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	3	Low	2	5	1	5	120	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.004.1A1.026	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	3	Low	2	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.017.1B1.129	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.023.1B1.170	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.026.1B1.188	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	SCU software setting	027	Systematic	Included	4	2	Low	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.029.1B1.210	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.033.1B1.236	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	SCU software setting	027	Systematic	Included	4	2	Low	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.035.2B1.254	The command is not followed due to failure in SCU to generate correct action.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.036.1B1.260	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.038.1B1.272	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	SCU software setting	027	Systematic	Included	4	2	Low	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.042.1B1.303	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.045.1B1.322	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	SCU software setting	027	Systematic	Included	4	2	Low	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.049.1B1.352	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	4	2	Low	3	1	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.052.1B1.371	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	SCU software setting	027	Systematic	Included	4	2	Low	3	3	5	5	120	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.001.2A0.007	Operator gives command to adjust set point of choke valve, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	3	Low	3	3	3	3	108	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.005.1B1.035	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	3	Medium	3	3	1	3	108	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.005.1B1.036	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	BP line pressure sensor miscalibration	004	Random	Included	4	3	Medium	3	3	3	3	108	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.OPE.010.1B1.074	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	3	Medium	3	3	1	3	108	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.010.1B1.075	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	NR line pressure sensor miscalibration	015	Random	Included	4	3	Medium	3	3	3	3	108	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.059.2B0.404	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Included	4	3	High	3	1	3	3	108	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.063.1A0.420	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Included	4	3	HIgh	3	1	3	3	108	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.064.2A0.430	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Included	4	3	High	3	1	3	3	108	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.067.2B0.443	SCM provides signal to open crossover valve correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	Low	3	3	1	3	108	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.068.1B0.446	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Included	4	3	Low	3	3	3	3	108	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.071.1A0.458	SCM generates correct command to open crossover valve, but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	Low	3	3	1	3	108	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.071.1B0.460	SCM receives spurious trip signal to close crossover valve due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	3	Low	3	3	3	3	108	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.073.2B0.473	SCM receives spurious trip signal to close crossover valve due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	3	Low	3	3	3	3	108	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.080.1A0.500	SCM generates correct command to open normal line isolation valve (XV-003 / XV-005), but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	Low	3	3	1	3	108	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.080.1B0.502	SCM receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	3	Low	3	3	3	3	108	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.089.1A0.542	SCM generates correct command to open bypass line isolation valve (XV-002 / XV-004), but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	Low	3	3	1	3	108	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.089.1B0.544	SCM receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	3	Low	3	3	3	3	108	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCU.053.1A1.375	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Included	4	3	Medium	3	1	3	3	108	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCU.054.2B0.383	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Included	4	3	Medium	3	1	3	3	108	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCU.058.1B1.396	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Included	4	3	High	3	1	3	3	108	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.004.2A0.030	Operator provides correct command of set point, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Screened Out	4	3	Low	3	1	3	3	108	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.004.2B0.031	Operator provides correct command of set point, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Screened Out	4	3	Low	3	1	3	3	108	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.SCM.077.1A0.488	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Screened Out	4	3	Low	3	1	3	3	108	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.082.2B0.515	SCM receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Screened Out	4	3	Low	3	1	3	3	108	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.086.1A0.530	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Screened Out	4	3	Low	3	1	3	3	108	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.091.2B0.557	SCM receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Screened Out	4	3	Low	3	1	3	3	108	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.OPE.006.1A1.044	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Included	4	2	High	4	3	3	3	96	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.006.1B1.046	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	2	High	4	3	1	3	96	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.006.1B1.047	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	NR line pressure sensor failure	014	Random	Included	4	2	High	4	3	1	3	96	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.008.1B0.061	Operator receives late information regarding the significant change of pressure differences in the SGB normal line.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Medium	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.OPE.011.1A1.083	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Included	4	2	High	4	3	3	3	96	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.011.1B1.085	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	2	High	4	3	1	3	96	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.011.2A0.088	Operator know the correct setpoint, but unknowingly input incorrect number.	Operator mistake	019	Random	Included	4	2	High	4	3	3	3	96	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.013.1B0.100	Operator receives late information regarding the significant change of pressure differences in the SGB normal line.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Medium	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.OPE.013.2A0.101	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Medium	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.SCM.060.1B0.408	Communication delay is present during the command from SCM to the variable speed drive.	Transmission line SCM - SGB transfer rate	035	Random	Included	4	4	High	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.SCM.061.1A1.411	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	High	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.SCM.061.2B1.415	SCM generates correct command to modify oil MP pump speed, but abrupt change happened due to loss of communication between SCM and the variable speed drive.	Transmission line SCM - SGB failure	033	Random	Included	4	2	High	4	3	1	3	96	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.062.1B0.416	SCM receives spurious trip signal to modify oil MP pump variable speed due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	2	High	4	3	3	3	96	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.062.1B1.417	SCM provides correct signal to modify oil MP pump variable speed, but abrupt change in variable speed drive signal returning the process to safe state happened due to failure of variable speed drive.	VSD failure & VSD setting	039	Random & Systematic	Included	4	2	High	4	3	3	3	96	* λ = 8.795E-5 (Oreda, 2002, p. 334) * Setting failure = Possible * Data from general pump topside * T = 10 year
SCE.SCM.065.1B1.433	Communication delay is present during the command from SCM to the variable speed drive.	Transmission line SCM - SGB transfer rate	035	Random	Included	4	4	High	2	3	3	3	96	* Transfer rate > 0.01 s

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.066.1A1.435	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	High	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.SCM.066.2B1.439	SCM generates correct command to modify water MP pump speed, but abrupt change happened due to loss of communication between SCM and the variable speed drive.	Transmission line SCM - SGB failure	033	Random	Included	4	2	High	4	3	1	3	96	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.067.1B0.440	SCM receives spurious trip signal to modify water MP pump variable speed due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	2	High	4	3	3	3	96	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.067.1B1.441	SCM provides correct signal to modify water MP pump variable speed, but abrupt change in variable speed drive signal returning the process to safe state happened due to failure of variable speed drive.	VSD failure & VSD setting	039	Random & Systematic	Included	4	2	High	4	3	3	3	96	* λ = 8.795E-5 (Oreda, 2002, p. 334) * Setting failure = Possible * Data from general pump topside * T = 10 year
SCE.SCM.071.2A0.461	Insufficient pressure to actuate the crossover valve.	Insufficient hydraulic pressure	009	Random	Included	4	4	Low	2	3	1	3	96	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.080.2A0.503	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005).	Insufficient hydraulic pressure	009	Random	Included	4	4	Low	2	3	1	3	96	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.089.2A0.545	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004).	Insufficient hydraulic pressure	009	Random	Included	4	4	Low	2	3	1	3	96	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.098.1A0.584	Communication delay is present during the command from SCU to SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	High	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.SCM.098.2B0.588	SCU receives late information regarding the command from the operator due to communication delay between operator and SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	High	2	3	3	3	96	* Transfer rate > 0.01 s
SCE.SCU.057.1A0.390	SCM generates correct command to modify choke valve opening, but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	2	Medium	4	3	1	3	96	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCU.057.1B0.392	SCM receives spurious trip signal to modify choke valve opening due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Included	4	2	Medium	4	3	3	3	96	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.OPE.020.1B1.148	Incorrect feedback about the actual condition of the system is received due to failure of SCU to generate correct information.	SCU failure	024	Random	Included	4	2	Low	4	3	1	3	96	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.045.2B0.324	Operator provides correct command to use SGB2 normal line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure	024	Random	Included	4	2	Low	4	3	1	3	96	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.007.1B1.056	Incorrect feedback about the active process line is received due to wrong HMI setting produced by SCU.	SCU software setting	027	Systematic	Screened Out	3	2	Low	3	1	5	5	90	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.007.2B0.057	Operator provides correct command to adjust set point of oil MP pump speed to the normal process line, but SCU proceed with incorrect process line.	SCU software setting	027	Systematic	Screened Out	3	2	Low	3	1	5	5	90	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.012.1B1.095	Incorrect feedback about the active process line is received due to wrong HMI setting produced by SCU.	SCU software setting	027	Systematic	Screened Out	3	2	Low	3	1	5	5	90	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.012.2B0.096	Operator provides correct command to adjust set point of water MP pump speed to the normal process line, but SCU proceed with incorrect process line.	SCU software setting	027	Systematic	Screened Out	3	2	Low	3	1	5	5	90	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.019.1B0.141	Operator receives late information regarding the process status in the SGB1 normal line.	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	032	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 1 s
SCE.OPE.019.2A0.142	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 0.01 s
SCE.OPE.025.1B0.181	Operator receives late information regarding the process status in the SGB1 normal line.	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	032	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 1 s

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.025.2A0.182	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 0.01 s
SCE.OPE.032.1B0.229	Operator receives late information regarding the process status in the SGB1 normal line.	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	032	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 1 s
SCE.OPE.032.2A0.230	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 0.01 s
SCE.OPE.037.1B0.265	Operator receives late information regarding the process status in the SGB1 bypass line.	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	032	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 1 s
SCE.OPE.037.2A0.266	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 0.01 s
SCE.OPE.044.1B0.315	Operator receives late information regarding the process status in the SGB1 bypass line.	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	032	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 1 s
SCE.OPE.044.2A0.316	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 0.01 s
SCE.OPE.051.1B0.364	Operator receives late information regarding the process status in the SGB1 bypass line.	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	032	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 1 s
SCE.OPE.051.2A0.365	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	5	3	5	80	* Transfer rate > 0.01 s
SCE.OPE.017.1A1.125	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	2	Low	2	1	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.020.1A1.145	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	Low	2	3	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.023.1A1.166	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	2	Low	2	1	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.023.1A1.167	Operator has too many process to be considered and mistakes one process to another.	Working condition	042	Random	Screened Out	4	2	Low	2	1	5	5	80	* Probability of event = E-5
SCE.OPE.026.1A1.185	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	Low	2	3	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.029.1A1.206	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	2	Low	2	1	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.033.1A1.233	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	Low	2	3	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.036.1A1.256	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	2	Low	2	1	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.038.1A1.269	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	Low	2	3	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.042.1A1.299	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	2	Low	2	1	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.045.1A1.319	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	Low	2	3	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.049.1A1.348	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	4	2	Low	2	1	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.052.1A1.368	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Included	4	2	Low	2	3	5	5	80	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.001.1B1.004	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	BP line pressure sensor failure	003	Random	Included	4	3	Low	2	3	1	3	72	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.002.1A1.012	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Included	4	3	Low	2	3	3	3	72	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.002.1B1.014	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	BP line pressure sensor failure	003	Random	Included	4	3	Low	2	3	1	3	72	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.002.2A0.017	Operator know the correct setpoint, but unknowingly input incorrect number.	Operator mistake	019	Random	Included	4	3	Low	2	3	3	3	72	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.006.1B1.048	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	NR line pressure sensor miscalibration	015	Random	Included	4	2	High	3	3	3	3	72	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.OPE.006.2A0.049	Operator know the correct setpoint, but unknowingly input incorrect number.	Operator mistake	019	Random	Included	4	3	Low	2	3	3	3	72	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.011.1B1.086	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	NR line pressure sensor miscalibration	015	Random	Included	4	2	High	3	3	3	3	72	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.SCM.068.1A0.444	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Included	4	3	Low	2	3	3	3	72	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.068.2B0.449	Failure happened in the crossover valve.	Crossover valve failure	007	Random	Included	4	3	Low	2	3	3	3	72	* λ = 9.022E-6 (Oreda, 2002, p. 823) * T = 10 year
SCE.SCM.068.2B1.450	Insufficient pressure to actuate the crossover valve in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Included	4	3	Low	2	3	1	3	72	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.068.2B1.451	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Included	4	3	Low	2	3	3	3	72	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCU.057.2B0.394	SCM provides correct signal to modify choke valve opening, but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	Choke valve failure & setting	006	Random & Systematic	Included	4	2	Medium	3	3	3	3	72	* λ = 2.533E-5 (Oreda, 2002, p. 833) * Setting failure = Possible * T = 10 year
SCE.OPE.017.2B0.130	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB1 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	4	2	Low	3	1	3	3	72	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.020.2A0.149	Operator provides correct command to use SGB1 bypass line, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	2	Low	3	3	3	3	72	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.020.2B0.150	Operator provides correct command to use SGB1 bypass line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	2	Low	3	3	3	3	72	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.OPE.023.2B0.171	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	4	2	Low	3	1	3	3	72	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.026.2A0.189	Operator provides correct command to use SGB2 normal line, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	2	Low	3	3	3	3	72	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.026.2B0.190	Operator provides correct command to use SGB2 normal line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	2	Low	3	3	3	3	72	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.OPE.029.2B0.211	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	4	2	Low	3	1	3	3	72	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.033.2A0.237	Operator provides correct command to use SGB2 bypass line, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	2	Low	3	3	3	3	72	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.033.2B0.238	Operator provides correct command to use SGB2 bypass line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	2	Low	3	3	3	3	72	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.OPE.036.2B0.261	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB1 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	4	2	Low	3	1	3	3	72	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.038.2A0.273	Operator provides correct command to use SGB1 normal line, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	2	Low	3	3	3	3	72	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.038.2B0.274	Operator provides correct command to use SGB1 normal line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	2	Low	3	3	3	3	72	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.OPE.042.2B0.304	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	4	2	Low	3	1	3	3	72	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.045.2A0.323	Operator provides correct command to use SGB2 normal line, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	2	Low	3	3	3	3	72	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.049.2B0.353	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	4	2	Low	3	1	3	3	72	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.052.2A0.372	Operator provides correct command to use SGB2 bypass line, but abrupt change happened due to loss of communication between operator HMI and SCU.	Transmission line HMI - SCU failure	029	Random	Included	4	2	Low	3	3	3	3	72	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.052.2B0.373	Operator provides correct command to use SGB2 bypass line, but abrupt change in SCU signal returning the system to safe state happened due to failure of SCU.	SCU failure & software setting	025	Random & Systematic	Included	4	2	Low	3	3	3	3	72	* λ = 1.828E-4 (Oreda, 2002, p. 811) * Setting failure = Possible * T = 10 year
SCE.SCM.076.2B0.487	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Screened Out	4	3	Low	2	1	3	3	72	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.077.1B0.490	Failure happened in the normal line isolation valve (XV-003 / XV-005).	NR line isolation valve (XV-003 / XV-005) failure	012	Random	Screened Out	4	3	Low	2	1	3	3	72	* λ = 9.022E-6 (Oreda, 2002, p. 823) * T = 10 year
SCE.SCM.077.2B0.493	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Screened Out	4	3	Low	2	1	3	3	72	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.082.2B1.516	Actuator receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	Transmission line SCM - SGB noise	034	Random	Screened Out	4	3	Low	2	1	3	3	72	* λ = 8.15E-6 (Oreda, 2002, p. 812) * Failure rate for both dynamic and static umbilical * 1/2 Jumper failure due to fail to transfer (Oreda, 2002, p. 813) * T = 10 year
SCE.SCM.085.2B0.529	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Screened Out	4	3	Low	2	1	3	3	72	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.086.1B0.532	Failure happened in the bypass line isolation valve (XV-002 / XV-004).	BP line isolation valve (XV-002 / XV-004) failure	001	Random	Screened Out	4	3	Low	2	1	3	3	72	* λ = 9.022E-6 (Oreda, 2002, p. 823) * T = 10 year
SCE.SCM.086.2B0.535	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Screened Out	4	3	Low	2	1	3	3	72	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.091.2B1.558	Actuator receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	Transmission line SCM - SGB noise	034	Random	Screened Out	4	3	Low	2	1	3	3	72	* λ = 8.15E-6 (Oreda, 2002, p. 812) * Failure rate for both dynamic and static umbilical * 1/2 Jumper failure due to fail to transfer (Oreda, 2002, p. 813) * T = 10 year
SCE.OPE.015.1B1.114	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	NR line pressure sensor miscalibration	015	Random	Included	4	3	Low	1	5	3	5	60	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.OPE.007.1A1.052	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Screened Out	3	2	Low	2	1	5	5	60	* Probability of event = E-5
SCE.OPE.007.1A1.053	Operator cannot clearly differentiate between normal process line and bypass process line.	Operator knowledge	018	Systematic	Screened Out	3	2	Low	2	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.012.1A1.091	Operator is under pressure due to too many responsibilities and process to be considered.	Working condition	042	Random	Screened Out	3	2	Low	2	1	5	5	60	* Probability of event = E-5
SCE.OPE.012.1A1.092	Operator cannot clearly differentiate between normal process line and bypass process line.	Operator knowledge	018	Systematic	Screened Out	3	2	Low	2	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.018.1B1.136	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	3	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.024.1B1.176	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.030.1B1.217	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	3	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.031.1B1.224	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.034.1B1.243	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.039.1B1.279	Incorrect feedback about the actual process line condition is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.041.1B1.296	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.043.1B1.310	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.047.1B1.338	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.048.1B1.345	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.050.1B1.359	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	2	Low	3	1	5	5	60	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.074.1B0.477	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	2	3	Low	3	3	3	3	54	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.SCM.083.1B0.519	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	2	3	Low	3	3	3	3	54	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.092.1B0.561	High load in the process memory due to too many process to be considered.	SCM hardware capability	022	Random	Included	2	3	Low	3	3	3	3	54	* λ = 1.294E-5 (Oreda, 2002, p. 811) * 18/206 Failure due to fail to function on demand & Erratic Output (Oreda, 2002, p. 813) * T = 10 Year
SCE.OPE.003.1B0.022	Operator receives late information regarding the pressure of hydrocarbon in the SGB bypass line.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.OPE.003.2A0.023	Communication delay is present during the command from operator to SCU.	Transmission line HMI - SCU transfer rate	031	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.OPE.009.1B1.068	Incorrect feedback about the actual pressure condition of the system is received due to failure of SCU to generate correct information.	SCU failure	024	Random	Included	4	3	Medium	4	1	1	1	48	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.014.1B1.107	Incorrect feedback about the actual pressure condition of the system is received due to failure of SCU to generate correct information.	SCU failure	024	Random	Included	4	3	Medium	4	1	1	1	48	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.059.1B1.402	SCM modifies oil MP pump variable speed opening correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	High	4	1	1	1	48	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.062.2B0.419	SCM modifies water MP pump variable speed, but the command is not received by the water MP pump (on SGB normal line).	Transmission line SCM - SGB failure	033	Random	Included	4	3	HIgh	4	1	1	1	48	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.063.2B1.427	SCM modifies water MP pump variable speed opening correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	High	4	1	1	1	48	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.069.1A0.452	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCM.070.1B0.456	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCM.077.2B1.495	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCM.079.1B1.498	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCM.086.2B1.537	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCM.088.1B1.540	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	Low	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCU.053.2A0.378	SCM modifies choke valve opening, but the command is not received by the choke valve (on SGB bypass line).	Transmission line SCM - SGB failure	033	Random	Included	4	3	Medium	4	1	1	1	48	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCU.054.1A0.380	Insufficient pressure to actuate the choke valve in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Included	4	3	Medium	4	1	1	1	48	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCU.054.1B0.381	SCM modifies choke valve opening correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Included	4	3	Medium	4	1	1	1	48	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCU.055.1A0.384	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	4	4	Medium	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCU.056.1A1.388	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	4	4	Medium	1	3	3	3	48	* Transfer rate > 0.01 s
SCE.SCU.058.2A0.397	SCM modifies oil MP pump variable speed, but the command is not received by the oil MP pump (on SGB normal line).	Transmission line SCM - SGB failure	033	Random	Included	4	3	High	4	1	1	1	48	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.OPE.017.1A1.126	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	4	2	Low	2	1	3	3	48	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.020.1B1.147	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	2	Low	2	3	1	3	48	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.026.1B1.187	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	2	Low	2	3	1	3	48	* λ = 4,996E-6 (Oreda, 2002, p. 811)

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.029.1A1.207	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	4	2	Low	2	1	3	3	48	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.033.1B1.235	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	2	Low	2	3	1	3	48	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.036.1A1.257	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	4	2	Low	2	1	3	3	48	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.038.1B1.271	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	2	Low	2	3	1	3	48	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.042.1A1.300	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	4	2	Low	2	1	3	3	48	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.045.1B1.321	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	2	Low	2	3	1	3	48	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.049.1A1.349	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	4	2	Low	2	1	3	3	48	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.052.1B1.370	Incorrect feedback about the actual condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Included	4	2	Low	2	3	1	3	48	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.016.1B1.122	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	1	High	4	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.018.1A1.132	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	3	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.022.1B1.163	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	1	High	4	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.028.1B1.203	Incorrect feedback about the actual pressure condition of the system is received due to wrong alarm setting in SCU.	SCU software setting	027	Systematic	Screened Out	2	1	High	4	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.OPE.030.1A1.213	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	3	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.031.1A1.220	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.034.1A1.240	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.039.1A1.276	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.041.1A1.292	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.043.1A1.306	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.047.1A1.334	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.048.1A1.341	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.050.1A1.355	Lack of understanding to the appropriate respond when facing the situation.	Operator knowledge	018	Systematic	Screened Out	2	2	Low	2	1	5	5	40	* Systematic error factor, not possible to assign frequency * Probability of operator inability to perform, given required knowledge is not available
SCE.OPE.001.1B1.005	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	BP line pressure sensor miscalibration	004	Random	Included	4	3	Low	1	3	3	3	36	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.OPE.002.1B1.015	Incorrect feedback about the actual pressure condition of the system is received due to wrong calibration of the sensor.	BP line pressure sensor miscalibration	004	Random	Included	4	3	Low	1	3	3	3	36	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.OPE.009.1B1.067	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	3	Medium	3	1	1	1	36	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.014.1B1.106	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Included	4	3	Medium	3	1	1	1	36	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.SCM.071.2B0.462	SCM provides correct signal to open crossover valve, but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	Crossover valve failure & setting	008	Random & Systematic	Included	4	3	Low	1	3	3	3	36	* λ = 9.022E-6 (Oreda, 2002, p. 823) * Setting failure = Possible * T = 10 year
SCE.SCM.080.2B0.504	SCM provides correct signal to open normal line isolation valve (XV-003 / XV-005), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	NR line isolation valve (XV-003 / XV-005) failure & setting	013	Random & Systematic	Included	4	3	Low	1	3	3	3	36	* λ = 9.022E-6 (Oreda, 2002, p. 823) * Setting failure = Possible * T = 10 year
SCE.SCM.089.2B0.546	SCM provides correct signal to open bypass line isolation valve (XV-002 / XV-004), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	BP line isolation valve (XV-002 / XV-004) failure & setting	002	Random	Included	4	3	Low	1	3	3	3	36	* λ = 9.022E-6 (Oreda, 2002, p. 823) * Setting failure = Possible * T = 10 year
SCE.OPE.004.1B1.029	Incorrect feedback about the actual pressure condition of the system is received due to failure of SCU.	BP line pressure sensor miscalibration	004	Random	Screened Out	4	3	Low	1	1	3	3	36	* λ = 1.070E-6 (Oreda, 2002, p. 811) * 3/14 Failure due to faulty signal (Oreda, 2002, p. 814) * T = 10 year
SCE.OPE.018.2B0.137	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB1 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	3	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.024.2B0.177	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.030.2B0.218	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	3	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.031.2B0.225	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.034.2A0.244	Operator gives command to change flow line from SGB1 bypass line to SGB1 normal line, but the command is not received by SCU. \	Transmission line HMI - SCU failure	029	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.039.2A0.280	Operator gives command to change flow line from SGB1 bypass line to SGB2 normal line, but the command is not received by SCU.	Transmission line HMI - SCU failure	029	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.041.2B0.297	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.043.2B0.311	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.047.2B0.339	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU failure	029	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * T = 10 year
SCE.OPE.048.2B0.346	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.050.2B0.360	SCU receives spurious trip signal to change flow line from SGB1 bypass line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.SCM.071.2B1.463	SCM provides signal to close crossover valve correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	2	2	Low	3	3	1	3	36	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.072.2B0.467	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Screened Out	2	2	Low	3	3	3	3	36	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.075.1A1.479	Insufficient pressure to actuate the crossover valve.	Insufficient hydraulic pressure	009	Random	Included	2	3	Low	2	3	1	3	36	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.075.1B0.480	SCM generates correct command to close crossover valve, but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	2	2	Low	3	3	1	3	36	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.075.2B1.483	SCM receives spurious trip signal to close crossover valve due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Screened Out	2	2	Low	3	3	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.076.1B0.484	SCM provides signal to open normal line isolation valve (XV-003 / XV-005) correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	4	3	Low	3	1	1	1	36	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.081.2B0.509	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.084.1A1.521	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005).	Insufficient hydraulic pressure	009	Random	Included	2	3	Low	2	3	1	3	36	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.084.1B0.522	SCM generates correct command to close normal line isolation valve (XV-003 / XV-005), but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	2	2	Low	3	3	1	3	36	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.084.2B1.525	SCM receives spurious trip signal to close normal line isolation valve (XV-003 / XV-005) due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Screened Out	2	2	Low	3	3	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.SCM.085.1B0.526	SCM provides signal to open bypass line isolation valve (XV-002 / XV-004) correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	4	3	Low	3	1	1	1	36	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.090.2B0.551	SCM does not receive command from SCU due to loss of communication between SCU and SCM.	Transmission line SCU - SCM failure	036	Random	Screened Out	2	2	Low	3	1	3	3	36	* λ = 3.76E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical T = 10 year
SCE.SCM.093.1A1.563	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004).	Insufficient hydraulic pressure	009	Random	Included	2	3	Low	2	3	1	3	36	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.093.1B0.564	SCM generates correct command to close bypass line isolation valve (XV-002 / XV-004), but abrupt change happened due to loss of communication between SCM and the actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	2	2	Low	3	3	1	3	36	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.093.2B1.567	SCM receives spurious trip signal to close bypass line isolation valve (XV-002 / XV-004) due to noise in the communication line.	Transmission line SCU - SCM noise	037	Random	Screened Out	2	2	Low	3	3	3	3	36	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813) T = 10 Year
SCE.OPE.004.1B1.028	Incorrect feedback about the actual pressure condition of the system is received due to failure of the sensor.	BP line pressure sensor failure	003	Random	Screened Out	4	3	Low	2	1	1	1	24	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.016.1A1.119	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	1	High	4	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.016.2B0.123	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB1 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	1	High	4	1	3	3	24	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.018.1A1.133	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	3	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.018.1B1.135	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	2	Low	2	3	1	3	24	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.022.1A1.160	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	1	High	4	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.022.2B0.164	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 normal line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	1	High	4	1	3	3	24	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.024.1A1.173	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.028.1A1.200	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	1	High	4	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.028.2B0.204	SCU receives spurious trip signal to change flow line from SGB1 normal line to SGB2 bypass line due to noise in the communication line.	Transmission line HMI - SCU noise	030	Random	Screened Out	2	1	High	4	1	3	3	24	* λ = 2.589E-5 (Oreda, 2002, p. 811) * Failure rate for both dynamic and static umbilical * 1/2 Dynamic umbilical failure due to fail to transfer (Oreda, 2002, p. 813) * 8/10 Static umbilical failure due to fail to transfer (Oreda, 2002, p. 813)
SCE.OPE.030.1A1.214	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	3	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.031.1A1.221	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.041.1A1.293	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.043.1A1.307	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.047.1A1.335	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.048.1A1.342	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.OPE.050.1A1.356	Operator has too many process to be considered and mistakes one process to another.	Operator mistake	019	Random	Screened Out	2	2	Low	2	1	3	3	24	* Probability of operator mistake * Assumed as possible to happen
SCE.SCM.072.1B0.464	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Screened Out	2	2	Low	2	3	3	3	24	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.073.1A0.468	Failure happened in the crossover valve.	Crossover valve failure	007	Random	Screened Out	2	2	Low	2	3	3	3	24	* λ = 9.022E-6 (Oreda, 2002, p. 823) * T = 10 year
SCE.SCM.073.1A1.469	Insufficient pressure to actuate the crossover valve in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Screened Out	2	2	Low	2	3	1	3	24	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.073.1B0.470	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Screened Out	2	2	Low	2	3	3	3	24	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.077.1B1.491	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005) in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Screened Out	4	3	Low	2	1	1	1	24	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.081.1B0.506	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Screened Out	2	2	Low	2	1	3	3	24	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.082.1A0.510	Failure happened in the normal line isolation valve (XV-003 / XV-005).	NR line isolation valve (XV-003 / XV-005) failure	012	Random	Screened Out	2	2	Low	2	1	3	3	24	* λ = 9.022E-6 (Oreda, 2002, p. 823) * T = 10 year
SCE.SCM.082.1B0.512	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Screened Out	2	2	Low	2	1	3	3	24	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.086.1B1.533	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004) in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Screened Out	4	3	Low	2	1	1	1	24	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.090.1B0.548	SCM does not process the command due to missing/wrong logic in the program.	SCM software setting	023	Systematic	Screened Out	2	2	Low	2	1	3	3	24	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.091.1A0.552	Failure happened in the bypass line isolation valve (XV-002 / XV-004).	BP line isolation valve (XV-002 / XV-004) failure	001	Random	Screened Out	2	2	Low	2	1	3	3	24	* λ = 9.022E-6 (Oreda, 2002, p. 823) * T = 10 year
SCE.SCM.091.1B0.554	SCM receives correct command, but generate a wrong signal due to wrong logic in the software.	SCM software setting	023	Systematic	Screened Out	2	2	Low	2	1	3	3	24	* Systematic error factor, not possible to assign frequency * Probability of undetected systematic error happening during devlopment = Possible
SCE.SCM.073.2B1.475	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	2	3	Low	1	3	3	3	18	* Transfer rate > 0.01 s
SCE.SCM.075.2A0.481	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	2	3	Low	1	3	3	3	18	* Transfer rate > 0.01 s
SCE.SCM.082.2B1.517	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	2	3	Low	1	3	3	3	18	* Transfer rate > 0.01 s
SCE.SCM.084.2A0.523	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	2	3	Low	1	3	3	3	18	* Transfer rate > 0.01 s
SCE.SCM.091.2B1.559	Communication delay is present during the command from SCM to the actuator.	Transmission line SCM - SGB transfer rate	035	Random	Included	2	3	Low	1	3	3	3	18	* Transfer rate > 0.01 s
SCE.SCM.093.2A0.565	SCM receives late information regarding the command from SCU due to communication delay between SCU and SCM.	Transmission line SCU - SCM transfer rate	038	Random	Included	2	3	Low	1	3	3	3	18	* Transfer rate > 0.01 s
SCE.OPE.017.1B1.128	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	4	2	Low	2	1	1	1	16	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.023.1B1.169	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	4	2	Low	2	1	1	1	16	* λ = 4,996E-6 (Oreda, 2002, p. 811)

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.029.1B1.209	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	4	2	Low	2	1	1	1	16	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.036.1B1.259	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	4	2	Low	2	1	1	1	16	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.039.2B1.282	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Screened Out	2	2	Low	4	1	1	1	16	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.042.1B1.302	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	4	2	Low	2	1	1	1	16	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.049.1B1.351	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	4	2	Low	2	1	1	1	16	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.030.1B1.216	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line & BP line pressure sensor failure	011	Random	Screened Out	2	2	Low	1	3	1	3	12	* λ = 2,496E-11 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.059.2B1.406	SCM think that the flow is flowing in the normal line, when it is not.	NR line pressure sensor failure	014	Random	Screened Out	3	2	Low	2	1	1	1	12	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.SCM.060.1A0.407	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	3	2	Low	2	1	1	1	12	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.SCM.064.1B0.429	SCM think that the flow is flowing in the normal line, when it is not.	NR line pressure sensor failure	014	Random	Screened Out	3	2	Low	2	1	1	1	12	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.SCM.065.1B0.432	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	3	2	Low	2	1	1	1	12	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.SCM.076.2A0.486	SCM provides correct signal to open crossover valve, but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	Crossover valve failure & setting	008	Random & Systematic	Screened Out	2	2	Low	1	3	3	3	12	* λ = 9.022E-6 (Oreda, 2002, p. 823) * Setting failure = Possible * T = 10 year
SCE.SCM.080.2B1.505	SCM provides signal to close normal line isolation valve (XV-003 / XV-005) correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	2	2	Low	3	1	1	1	12	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.085.2A0.528	SCM provides correct signal to open normal line isolation valve (XV-003 / XV-005), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	NR line isolation valve (XV-003 / XV-005) failure & setting	013	Random & Systematic	Screened Out	2	2	Low	1	3	3	3	12	* λ = 9.022E-6 (Oreda, 2002, p. 823) * Setting failure = Possible * T = 10 year
SCE.SCM.089.2B1.547	SCM provides signal to close bypass line isolation valve (XV-002 / XV-004) correctly but is not received due to loss of communication line between SCM and actuator.	Transmission line SCM - SGB failure	033	Random	Screened Out	2	2	Low	3	1	1	1	12	* λ = 1.603E-5 (Oreda, 2002, p. 812) * Failure rate for power/signal jumper * T = 10 year
SCE.SCM.094.2A0.570	SCM provides correct signal to open bypass line isolation valve (XV-002 / XV-004), but abrupt change in actuator signal returning the process to safe state happened due to failure of actuator.	BP line isolation valve (XV-002 / XV-004) failure & setting	002	Random	Screened Out	2	2	Low	1	3	3	3	12	* λ = 9.022E-6 (Oreda, 2002, p. 823) * Setting failure = Possible * T = 10 year
SCE.OPE.015.2B1.117	The command is not followed due to failure in SCU to generate correct action.	SCU failure	024	Random	Screened Out	2	1	High	5	1	1	1	10	* λ = 1.828E-4 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.016.1B1.121	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	1	High	4	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.022.1B1.162	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	1	High	4	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.024.1B1.175	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.028.1B1.202	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	2	1	High	4	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.031.1B1.223	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.034.1B1.242	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.039.1B1.278	Incorrect feedback about the actual process line condition is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.041.1B1.295	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.043.1B1.309	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line pressure sensor failure	014	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811)
SCE.OPE.048.1B1.344	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.OPE.050.1B1.358	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	BP line pressure sensor failure	003	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 4,996E-6 (Oreda, 2002, p. 811) * T = 10 Year
SCE.SCM.082.1A1.511	Insufficient pressure to actuate the normal line isolation valve (XV-003 / XV-005) in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.SCM.091.1A1.553	Insufficient pressure to actuate the bypass line isolation valve (XV-002 / XV-004) in the hydraulic accumulator.	Insufficient hydraulic pressure	009	Random	Screened Out	2	2	Low	2	1	1	1	8	* λ = 7.976E-6 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.007.1B1.055	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	NR line & BP line pressure sensor failure	011	Random	Screened Out	3	2	Low	1	1	1	1	6	* λ = 2,496E-11 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.012.1B1.094	Incorrect feedback about the active process line is received due to failure of the sensor to generate correct information.	NR line & BP line pressure sensor failure	011	Random	Screened Out	3	2	Low	1	1	1	1	6	* λ = 2,496E-11 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.047.1B1.337	Incorrect feedback about the actual process condition of the system is received due to failure of the sensor to generate correct information.	NR line & BP line pressure sensor failure	011	Random	Screened Out	2	2	Low	1	1	1	1	4	* λ = 2,496E-11 (Oreda, 2002, p. 811) * T = 10 year
SCE.OPE.001.1A0.001	Operator understand that there is significant change of pressure of hydrocarbon in the SGB bypass line, but does not provide set point adjust-ment of choke valve.				Included	4	3	Low		3			0	* Unrefined scenario
SCE.OPE.001.1B0.003	Operator believes that there is no change of pressure of hydrocarbon in the SGB bypass line, but it is not.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.OPE.001.2B0.008	SCU receives the command to adjust set point of choke valve, but it is not followed.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.OPE.002.1A0.010	Operator understands the current pressure status in the SGB bypass line, but provides incorrect set point.				Included	4	3	Low		3			0	* Unrefined scenario
SCE.OPE.002.1B0.013	Operator receives wrong information regarding the pressure of hydrocarbon in the SGB bypass line.				Included	4	3	Low		3			0	* Unrefined scenario
SCE.OPE.003.1A0.019	Operator understands the current pressure status in the SGB bypass line, but takes long time to provide actions.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.OPE.005.1A0.032	Operator understand that there is significant change of hydrocarbon pressure differences in the SGB normal line, but does not provide set point adjustment of oil MP pump speed.				Included	4	3	Medium		3		3	0	* Unrefined scenario
SCE.OPE.005.1B0.034	Operator believes that there is significant change of hydrocarbon pressure differences in the SGB normal line, but it is not.				Included	4	3	Medium		3		3	0	* Unrefined scenario
SCE.OPE.005.2B0.039	SCU receives the command to adjust set point of oil MP pump speed, but it is not followed.				Included	4	3	Medium		3		3	0	* Unrefined scenario
SCE.OPE.006.1A0.042	Operator understands the current pressure differences status in the SGB normal line, but provides incorrect set point.				Included	4	2	High		3		3	0	* Unrefined scenario
SCE.OPE.006.1B0.045	Operator receives wrong information regarding the pressure differences of hydrocarbon in the SGB normal line.				Included	4	2	High		3		3	0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.008.1A0.058	Operator understands there is significant change of pressure differences in the SGB normal line, but takes long time to provide actions.				Included	4	4	Medium		3		3	0	* Unrefined scenario
SCE.OPE.009.1A0.064	Operator decided to change the set point before there is new change of pressure differences in the SGB normal line.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.OPE.009.1B0.066	Operator believes that there is new change of pressure differences in the SGB normal line, but it is not.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.OPE.010.1A0.071	Operator understand that there is significant change of hydrocarbon pressure differences in the SGB normal line, but does not provide set point adjustment of water MP pump speed.				Included	4	3	Medium		3		3	0	* Unrefined scenario
SCE.OPE.010.1B0.073	Operator believes that there is significant change of hydrocarbon pressure differences in the SGB normal line, but it is not.				Included	4	3	Medium		3		3	0	* Unrefined scenario
SCE.OPE.010.2B0.078	SCU receives the command to adjust set point of water MP pump speed, but it is not followed.				Included	4	3	Medium		3		3	0	* Unrefined scenario
SCE.OPE.011.1A0.081	Operator understands the current pressure differences status in the SGB normal line, but provides incorrect set point.				Included	4	2	High		3		3	0	* Unrefined scenario
SCE.OPE.011.1B0.084	Operator receives wrong information regarding the pressure differences of hydrocarbon in the SGB normal line.				Included	4	2	High		3		3	0	* Unrefined scenario
SCE.OPE.013.1A0.097	Operator understands there is significant change of pressure differences in the SGB normal line, but takes long time to provide actions.				Included	4	4	Medium		3		3	0	* Unrefined scenario
SCE.OPE.014.1A0.103	Operator decided to change the set point before there is new change of pressure differences in the SGB normal line.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.OPE.014.1B0.105	Operator believes that there is new change of pressure differences in the SGB normal line, but it is not.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.OPE.015.1A0.110	Operator understand that SGB1 normal line is faulty, but does not provide command to change flow line from SGB1 normal line to SGB1 bypass line.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.015.1B0.112	Operator believes that SGB1 normal line is normal, but it is not.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.015.2B0.116	SCU receives the command to change flow line from SGB1 normal line to SGB1 bypass line, but it is not followed.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.019.1A0.138	Operator understands the current process status in the SGB1 normal line, but takes long time to provide actions.				Included	4	4	Low		5		5	0	* Unrefined scenario
SCE.OPE.021.1A0.151	Operator understand that SGB1 normal line is faulty, but does not provide command to change flow line from SGB1 normal line to SGB2 normal line.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.021.1B0.153	Operator believes that SGB1 normal line is normal, but it is not.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.021.2B0.157	SCU receives the command to change flow line from SGB1 normal line to SGB2 normal line, but it is not followed.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.025.1A0.178	Operator understands the current process status in the SGB1 normal line, but takes long time to provide actions.				Included	4	4	Low		5		5	0	* Unrefined scenario
SCE.OPE.027.1A0.191	Operator understand that SGB1 normal line is faulty, but does not provide command to change flow line from SGB1 normal line to SGB2 bypass line.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.027.1B0.193	Operator believes that SGB1 normal line is normal, but it is not.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.027.2B0.197	SCU receives the command to change flow line from SGB1 normal line to SGB2 bypass line, but it is not followed.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.032.1A0.226	Operator understands the current process status in the SGB1 normal line, but takes long time to provide actions.				Included	4	4	Low		5		5	0	* Unrefined scenario
SCE.OPE.035.1A0.247	Operator understand that SGB1 bypass line is faulty, but does not provide command to change flow line from SGB1 bypass line to SGB1 normal line.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.035.1B0.249	Operator believes that SGB1 bypass line is normal, but it is not.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.035.2B0.253	SCU receives the command to change flow line from SGB1 bypass line to SGB1 normal line, but it is not followed.				Included	4	3	Low		5		5	0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.037.1A0.262	Operator understands the current process status in the SGB1 bypass line, but takes long time to provide actions.				Included	4	4	Low		5		5	0	* Unrefined scenario
SCE.OPE.040.1A0.283	Operator understand that SGB1 bypass line is faulty, but does not provide command to change flow line from SGB1 bypass line to SGB2 normal line.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.040.1B0.285	Operator believes that SGB1 bypass line is normal, but it is not.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.040.2B0.289	SCU receives the command to change flow line from SGB1 bypass line to SGB2 normal line, but it is not followed.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.044.1A0.312	Operator understands the current process status in the SGB1 bypass line, but takes long time to provide actions.				Included	4	4	Low		5		5	0	* Unrefined scenario
SCE.OPE.046.1A0.325	Operator understand that SGB1 bypass line is faulty, but does not provide command to change flow line from SGB1 bypass line to SGB2 bypass line.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.046.1B0.327	Operator believes that SGB1 bypass line is normal, but it is not.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.046.2B0.331	SCU receives the command to change flow line from SGB1 bypass line to SGB2 bypass line, but it is not followed.				Included	4	3	Low		5		5	0	* Unrefined scenario
SCE.OPE.051.1A0.361	Operator understands the current process status in the SGB1 bypass line, but takes long time to provide actions.				Included	4	4	Low		5		5	0	* Unrefined scenario
SCE.SCM.059.1A0.399	SCM generates signal to modify choke valve opening correctly, but it is not followed.				Included	4	3	High		1		1	0	* Unrefined scenario
SCE.SCM.061.1B0.412	Variable speed drive delays in the processing of command by SCM.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.061.2A0.413	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.062.2A0.418	SCM believes that the command to modify oil MP pump variable speed is stopped, but it is not.				Included	4	2	High		3		3	0	* Unrefined scenario
SCE.SCM.063.1A1.421	SCM does not receive the command from SCU to modify water MP pump variable speed.				Included	4	3	HIgh		1		1	0	* Unrefined scenario
SCE.SCM.063.1B1.423	SCM generates signal to modify choke valve opening correctly, but it is not followed.				Included	4	3	HIgh		1		1	0	* Unrefined scenario
SCE.SCM.063.2A0.424	SCM receives command from SCU, but it does not modify the water MP pump variable speed.				Included	4	3	HIgh		1		1	0	* Unrefined scenario
SCE.SCM.066.1B0.436	Variable speed drive delays in the processing of command by SCM.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.066.2A0.437	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.067.2A0.442	SCM believes that the command to modify water MP pump variable speed is stopped, but it is not.				Included	4	2	High		3		3	0	* Unrefined scenario
SCE.SCM.068.1A1.445	SCM does not receive the command from SCU to open crossover valve.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.SCM.068.1B1.447	SCM generates signal to open crossover valve correctly, but it is not followed.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.SCM.068.2A0.448	SCM receives command from SCU, but it does not open the crossover valve.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.SCM.069.1B0.453	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.SCM.070.1B1.457	Actuator delays in the processing of command by SCM.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.SCM.071.1A1.459	SCM believes that the command to open crossover valve is changed, but it is not.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.SCM.073.2B1.474	Actuator receives spurious trip signal to close crossover valve due to noise in the communication line.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.SCM.078.1A0.496	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.SCM.079.2B0.499	Actuator delays in the processing of command by SCM.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.SCM.080.1A1.501	SCM believes that the command to open normal line isolation valve (XV-003 / XV-005) is changed, but it is not.				Included	4	3	Low		3		3	0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.087.1A0.538	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.SCM.088.2B0.541	Actuator delays in the processing of command by SCM.				Included	4	4	Low		3		3	0	* Unrefined scenario
SCE.SCM.089.1A1.543	SCM believes that the command to open bypass line isolation valve (XV-002 / XV-004) is changed, but it is not.				Included	4	3	Low		3		3	0	* Unrefined scenario
SCE.SCM.094.1B1.569	SCU receives command from the operator, but it does not distribute the control action to SCM.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.095.2A0.576	SCU does not receive the command from the operator to distribute control.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.097.1B1.582	SCU believes that there is command, but it is not.				Included	4	3	High		3		3	0	* Unrefined scenario
SCE.SCM.098.1A1.585	SCU understands that there is command from the operator, but takes long time to distribute signal.				Included	4	4	High		3		3	0	* Unrefined scenario
SCE.SCM.099.1B0.590	SCU believes that the command to distribute control actions is stopped, but it is not.				Included	4	3	High		3		3	0	* Unrefined scenario
SCE.SCU.053.1A0.374	SCM receives command from SCU, but it does not modify the choke valve opening.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.SCU.053.1B0.376	SCM does not receive the command from SCU to modify choke valve opening.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.SCU.053.2B0.379	SCM generates signal to modify choke valve opening correctly, but it is not followed.				Included	4	3	Medium		1		1	0	* Unrefined scenario
SCE.SCU.055.1B0.385	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	4	4	Medium		3		3	0	* Unrefined scenario
SCE.SCU.056.1B0.389	Actuator delays in the processing of command by SCM.				Included	4	4	Medium		3		3	0	* Unrefined scenario
SCE.SCU.057.1A1.391	SCM believes that the command to modify choke valve opening is stopped, but it is not.				Included	4	2	Medium		3		3	0	* Unrefined scenario
SCE.SCU.058.1B0.395	SCM receives command from SCU, but it does not modify the oil MP pump variable speed.				Included	4	3	High		1		1	0	* Unrefined scenario
SCE.SCU.058.2B0.398	SCM does not receive the command from SCU to modify oil MP pump variable speed.				Included	4	3	High		1		1	0	* Unrefined scenario
SCE.OPE.004.1A0.025	Operator decided to change the set point before the pressure return to the normal condition.				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.OPE.004.1B0.027	Operator believes that the pressure of hydrocarbon in the SGB bypass line has returned to normal, but it is not.				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.OPE.007.1A0.051	Operator think that the flow is flowing in the normal line, when it is not.				Screened Out	3	2	Low		1			0	* Unrefined scenario
SCE.OPE.007.1B0.054	Operator receives wrong information regarding the current active process line in the SGB.				Screened Out	3	2	Low		1			0	* Unrefined scenario
SCE.OPE.012.1A0.090	Operator think that the flow is flowing in the normal line, when it is not.				Screened Out	3	2	Low		1			0	* Unrefined scenario
SCE.OPE.012.1B0.093	Operator receives wrong information regarding the current active process line in the SGB.				Screened Out	3	2	Low		1			0	* Unrefined scenario
SCE.OPE.016.1A0.118	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.				Screened Out	2	1	High		1			0	* Unrefined scenario
SCE.OPE.016.1B0.120	Operator receives wrong information regarding the current process status in the SGB1 normal line.				Screened Out	2	1	High		1			0	* Unrefined scenario
SCE.OPE.017.1A0.124	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.				Screened Out	4	2	Low		1			0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.017.1B0.127	Operator receives wrong information regarding the current process status in the SGB1 bypass line.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.018.1A0.131	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.OPE.018.1B0.134	Operator receives wrong information regarding the current process status in the SGB1 normal line and SGB2 normal line.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.OPE.020.1A0.144	Operator decided to change the process line before the target process line return to the normal condition.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.020.1B0.146	Operator believes that the SGB1 normal line has returned to normal, but it is not.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.022.1A0.159	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.				Screened Out	2	1	High		1			0	* Unrefined scenario
SCE.OPE.022.1B0.161	Operator receives wrong information regarding the current process status in the SGB1 normal line.				Screened Out	2	1	High		1			0	* Unrefined scenario
SCE.OPE.023.1A0.165	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.023.1B0.168	Operator receives wrong information regarding the current process status in the SGB2 normal line.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.024.1A0.172	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.024.1B0.174	Operator receives wrong information regarding the current process status in the SGB2 normal line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.026.1A0.184	Operator decided to change the process line before the target process line return to the normal condition.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.026.1B0.186	Operator believes that the SGB1 normal line has returned to normal, but it is not.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.028.1A0.199	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.				Screened Out	2	1	High		1			0	* Unrefined scenario
SCE.OPE.028.1B0.201	Operator receives wrong information regarding the current process status in the SGB2 bypass line.				Screened Out	2	1	High		1			0	* Unrefined scenario
SCE.OPE.029.1A0.205	Operator understands the current process status in the SGB2 bypass line, but made incorrect decisions.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.029.1B0.208	Operator receives wrong information regarding the current process status in the SGB2 bypass line.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.030.1A0.212	Operator understands the current process status in the SGB1 bypass line or SGB2 normal line, but made incorrect decisions.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.OPE.030.1B0.215	Operator receives wrong information regarding the current process status in the SGB1 bypass line or SGB2 normal line.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.OPE.031.1A0.219	Operator understands the current process status in the SGB2 bypass line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.031.1B0.222	Operator receives wrong information regarding the current process status in the SGB2 bypass line.				Screened Out	2	2	Low		1			0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.033.1A0.232	Operator decided to change the process line before the target process line return to the normal condition.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.033.1B0.234	Operator believes that the SGB1 normal line has returned to normal, but it is not.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.034.1A0.239	Operator understand that SGB1 normal line is normal, but does not provide command to change flow line from SGB1 bypass line to SGB1 normal line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.034.1B0.241	Operator believes that SGB1 normal line is faulty, but it is not.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.034.2B0.245	SCU receives the command to change flow line from SGB1 bypass line to SGB1 normal line, but it is not followed.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.036.1A0.255	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.036.1B0.258	Operator receives wrong information regarding the current process status in the SGB1 normal line.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.038.1A0.268	Operator decided to change the process line before the target process line return to the normal condition.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.038.1B0.270	Operator believes that the SGB1 bypass line has returned to normal, but it is not.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.039.1A0.275	Operator understand that SGB2 normal line is normal, but does not provide command to change flow line from SGB1 bypass line to SGB2 normal line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.039.1B0.277	Operator believes that SGB2 normal line is faulty, but it is not.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.039.2B0.281	SCU receives the command to change flow line from SGB1 bypass line to SGB2 normal line, but it is not followed.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.041.1A0.291	Operator understands the current process status in the SGB1 normal line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.041.1B0.294	Operator receives wrong information regarding the current process status in the SGB1 normal line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.042.1A0.298	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.042.1B0.301	Operator receives wrong information regarding the current process status in the SGB2 normal line.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.043.1A0.305	Operator understands the current process status in the SGB2 normal line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.043.1B0.308	Operator receives wrong information regarding the current process status in the SGB2 normal line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.045.1A0.318	Operator decided to change the process line before the target process line return to the normal condition.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.045.1B0.320	Operator believes that the SGB1 bypass line has returned to normal, but it is not.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.047.1A0.333	Operator understands the current process status in all SGB process line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.047.1B0.336	Operator receives wrong information regarding the current process status in the all SGB process line.				Screened Out	2	2	Low		1			0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.OPE.048.1A0.340	Operator understands the current process status in SGB2 bypass line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.048.1B0.343	Operator receives wrong information regarding the current process status in the SGB2 bypass line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.049.1A0.347	Operator understands the current process status in SGB2 bypass line, but made incorrect decisions.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.049.1B0.350	Operator receives wrong information regarding the current process status in the SGB2 bypass line.				Screened Out	4	2	Low		1			0	* Unrefined scenario
SCE.OPE.050.1A0.354	Operator understands the current process status in SGB2 bypass line, but made incorrect decisions.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.050.1B0.357	Operator receives wrong information regarding the current process status in the SGB2 bypass line.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.OPE.052.1A0.367	Operator decided to change the process line before the target process line return to the normal condition.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.OPE.052.1B0.369	Operator believes that the SGB1 bypass line has returned to normal, but it is not.				Included	4	2	Low		3			0	* Unrefined scenario
SCE.SCM.060.2A0.409	SCM receives wrong information regarding the current active process line in the SGB.				Screened Out	3	2	Low		1			0	* Unrefined scenario
SCE.SCM.065.1A0.431	SCM receives wrong information regarding the current active process line in the SGB.				Screened Out	3	2	Low		1			0	* Unrefined scenario
SCE.SCM.072.1B1.465	SCM does not receive the command from SCU to close crossover valve.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.SCM.072.2A0.466	SCM receives command from SCU, but it does not close the crossover valve.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.SCM.073.1B1.471	SCM receives wrong command from SCU.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.SCM.073.2A0.472	SCM generates signal to close crossover valve correctly, but it is not followed.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.SCM.074.1A0.476	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	2	3	Low		3			0	* Unrefined scenario
SCE.SCM.075.1A0.478	Actuator delays in the processing of command by SCM.				Included	2	3	Low		3			0	* Unrefined scenario
SCE.SCM.075.2B0.482	SCM believes that the command to close crossover valve is changed, but it is not.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.SCM.076.1B1.485	SCM receives command from SCU, but it does not open the normal line isolation valve (XV-003 / XV-005)				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.SCM.077.1A1.489	SCM generates signal to open normal line isolation valve (XV-003 / XV-005) correctly, but it is not followed.				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.SCM.077.2A0.492	SCM does not receive the command from SCU to open normal line isolation valve (XV-003 / XV-005).				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.SCM.081.1B1.507	SCM does not receive the command from SCU to close normal line isolation valve (XV-003 / XV-005).				Screened Out	2	2	Low		1			0	* Unrefined scenario

Sce Tag	Scenario	Causal Factor	CF Tag	CF Type	UCA Assessment	Severity	Mitigation	Cond. Event Likelihood	Scenario Likelihood	UCA. Knowledge	CF Knowledge	Scenario Knowledge	SCRPN	Assumption
SCE.SCM.081.2A0.508	SCM receives command from SCU, but it does not close the normal line isolation valve (XV-003 / XV-005).				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.082.1B1.513	SCM receives wrong command from SCU.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.082.2A0.514	SCM generates signal to close normal line isolation valve (XV-003 / XV-005) correctly, but it is not followed.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.083.1A0.518	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	2	3	Low		3			0	* Unrefined scenario
SCE.SCM.084.1A0.520	Actuator delays in the processing of command by SCM.				Included	2	3	Low		3			0	* Unrefined scenario
SCE.SCM.084.2B0.524	SCM believes that the command to close normal line isolation valve (XV-003 / XV-005) is changed, but it is not.				Screened Out	2	2	Low		3			0	* Unrefined scenario
SCE.SCM.085.1B1.527	SCM receives command from SCU, but it does not open the bypass line isolation valve (XV-002 / XV-004).				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.SCM.086.1A1.531	SCM generates signal to open bypass line isolation valve (XV-002 / XV-004) correctly, but it is not followed.				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.SCM.086.2A0.534	SCM does not receive the command from SCU to open bypass line isolation valve (XV-002 / XV-004).				Screened Out	4	3	Low		1			0	* Unrefined scenario
SCE.SCM.090.1B1.549	SCM does not receive the command from SCU to close bypass line isolation valve (XV-002 / XV-004).				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.090.2A0.550	SCM receives command from SCU, but it does not close the bypass line isolation valve (XV-002 / XV-004).				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.091.1B1.555	SCM receives wrong command from SCU.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.091.2A0.556	SCM generates signal to close bypass line isolation valve (XV-002 / XV-004) correctly, but it is not followed.				Screened Out	2	2	Low		1			0	* Unrefined scenario
SCE.SCM.092.1A0.560	SCM understands that there is command from the operator, but takes long time to generate signal.				Included	2	3	Low		3			0	* Unrefined scenario
SCE.SCM.093.1A0.562	Actuator delays in the processing of command by SCM.				Included	2	3	Low		3			0	* Unrefined scenario
SCE.SCM.093.2B0.566	SCM believes that the command to close bypass line isolation valve (XV-002 / XV-004) is changed, but it is not.				Screened Out	2	2	Low		3			0	* Unrefined scenario

Appendix F

Causal Factor Ranking Results

Causal Factor Ranking

CF Tag	Causal Factor	Hierarchical Control System	CF Type	Included Scenario	Max SCRPN	Screened Out Scenario	Max SCRPN
027	SCU software setting	SCU	Systematic	30	320	27	180
020	SCM failure	SCM	Random	1	240	0	0
024	SCU failure	SCU	Random	11	240	2	16
026	SCU hardware capability	SCU	Random	10	240	0	0
028	Task procedure	OPE	Systematic	9	240	0	0
042	Working condition	OPE	Random	9	240	3	80
009	Insufficient hydraulic pressure	SGB NR / SGB BP	Random	9	192	5	24
019	Operator mistake	OPE	Random	8	192	17	48
022	SCM hardware capability	SCM	Random	10	192	0	0
029	Transmission line HMI - SCU failure	OPE - SCU	Random	19	192	4	108
036	Transmission line SCU - SCM failure	SCU - SCM	Random	7	192	5	108
016	Oil MP pump failure	SGB NR	Random	1	180	0	0
017	Oil MP pump vsd failure	SGB NR	Random	1	180	0	0
018	Operator knowledge	OPE	Systematic	20	180	19	120
040	Water MP pump failure	SGB NR	Random	1	180	0	0
041	Water MP pump vsd failure	SGB NR	Random	1	180	0	0
005	Choke valve failure	SGB BP	Random	1	144	0	0
010	Insufficient power supply	SGB NR / SGB BP	Random	2	144	0	0
021	SCM failure & software setting	SCM	Random & Systematic	1	144	0	0
023	SCM software setting	SCM	Systematic	9	144	10	72
025	SCU failure & software setting	SCU	Random & Systematic	7	144	1	108
030	Transmission line HMI - SCU Noise	OPE - SCU	Random	2	144	17	72
003	BP line pressure sensor failure	SGB BP	Random	9	120	8	24
014	NR line pressure sensor failure	SGB NR	Random	12	120	15	24
004	BP line pressure sensor miscalibration	SGB BP	Random	3	108	1	36
015	NR line pressure sensor miscalibration	SGB NR	Random	4	108	0	0
033	Transmission line SCM - SGB failure	SCM - SGB	Random	13	108	8	36
037	Transmission line SCU - SCM Noise	SCU - SCM	Random	7	108	5	108
031	Transmission line HMI - SCU transfer rate	OPE - SCU	Random	12	96	0	0
035	Transmission line SCM - SGB transfer rate	SCM - SGB	Random	9	96	0	0
038	Transmission line SCU - SCM transfer rate	SCU - SCM	Random	10	96	0	0
039	VSD failure & VSD setting	SGB NR	Random & Systematic	2	96	0	0
032	Transmission line HMI - SCU, SCU - SCM & SCM - SGB transfer rate	OPE - SCU / SCU - SCM / SCM - SGB	Random	6	80	0	0
006	Choke valve failure & setting	SGB BP	Random & Systematic	1	72	0	0
007	Crossover valve failure	SGB XOV	Random	1	72	1	24
002	BP line isolation valve (XV-002 / XV-004) failure & setting	SGB BP	Random	1	36	1	12

CF Tag	Causal Factor	Hierarchical Control System	CF Type	Included Scenario	Max SCRPN	Screened Out Scenario	Max SCRPN
008	Crossover valve failure & setting	SGB XOV	Random & Systematic	1	36	1	12
013	NR line isolation valve (XV-003 / XV-005) failure & setting	SGB NR	Random & Systematic	1	36	1	12
001	BP line isolation valve (XV-002 / XV-004) failure	SGB BP	Random	0	0	2	72
011	NR line & BP line pressure sensor failure	SBG NR / SGB BP	Random	0	0	4	12
012	NR line isolation valve (XV-003 / XV-005) failure	SGB NR	Random	0	0	2	72
034	Transmission line SCM - SGB Noise	SCM - SGB	Random	0	0	2	72

Bibliography

Abrecht, B. R. (2016). Systems theoretic process analysis applied to an offshore supply vessel dynamic positioning system. Master's thesis, Massachusetts Institute of Technology.

Aps, R., Fetissov, M., Goerlandt, F., Kujala, P., and Piel, A. (2017). Systems-theoretic process analysis of maritime traffic safety management in the gulf of finland (baltic sea). *Procedia Engineering*, 179:2–12.

Berner, C. and Flage, R. (2016). Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions. *Reliability Engineering & System Safety*, 151:46–59.

Board, J. P. L. U. S. R. and Casani, J. (2000). *Report on the loss of the mars polar lander and deep space 2 missions*. Jet Propulsion Laboratory, California Institute of Technology.

Bogard, W. (1989). The bhopal tragedy.

Bowles, J. B. (2003). An assessment of rpn prioritization in a failure modes effects and criticality analysis. In *Reliability and Maintainability Symposium, 2003. Annual*, pages 380–386. IEEE.

BP (2010). *Deepwater horizon accident investigation report*. BP.

Braglia, M. (2000). Mafma: multi-attribute failure mode analysis. *International Journal of Quality & Reliability Management*, 17(9):1017–1033.

Braglia, M. and Bevilacqua, M. (2000). Fuzzy modelling and analytical hierarchy processing as a means of quantifying risk levels associated with failure modes in production systems. *Technology, Law and Insurance*, 5(3-4):125–134.

Budde, S. F. (2012). Modeling blowouts during drilling using stamp and stpa. Master's thesis, Norges Teknisk-Naturvitenskapelige Universitet.

Chang, C.-L., Wei, C.-C., and Lee, Y.-H. (1999). Failure mode and effects analysis using fuzzy method and grey theory. *Kybernetes*, 28(9):1072–1080.

Chen, J. K. (2007). Utility priority number evaluation for fmea. *Journal of failure analysis and Prevention*, 7(5):321–328.

Davidson, G. and Labib, A. (2003). Learning from failures: design improvements using a multiple criteria decision-making process. *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, 217(4):207–216.

Flage, R. and Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability: Theory & Applications*, 4(2-1 (13)).

Folse, S. A. (2017). *Systems-theoretic process analysis of small unmanned aerial system use at Edwards Air Force Base*. PhD thesis, Massachusetts Institute of Technology.

Hafver, A., Eldevik, S., Jakopanec, I., Drugan, O. V., Pedersen, F. B., Flage, R., and Aven, T. (2017). Risk-based versus control-based safety philosophy in the context of complex systems. In *ESREL 2017 (Portoroz, Slovenia, 18-22 June, 2017)*.

Hardy, K. and Guarnieri, F. (2011). Using a systemic model of accident for improving innovative technologies: Application and limitations of the stamp model to a process for treatment of contaminated substances. In *The 15th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2011*.

Hoel, F. (2012). Modeling process leaks offshore using stamp and stpa.

Hollnagel, E. and Goteman, O. (2004). The functional resonance accident model. *Proceedings of cognitive system engineering in process plant*, 2004:155–161.

ISO (2002). Bs en iso 17776: 2002 petroleum and natural gas industries—offshore production installations—guidelines on tools and techniques for hazard identification and risk assessment.

ISO (2009). 31000: 2009 risk management—principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*.

Johansen, I. L. (2010). Foundations of risk assessment. Master's thesis, Norges Teknisk-Naturvitenskapelige Universitet.

Kaplan, S. and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, 1(1):11–27.

Lee, D.-A., Lee, J.-S., Cheon, S.-W., and Yoo, J. (2013). Application of system-theoretic process analysis to engineered safety features-component control system. In *Proc. of the 37th Enlarged Halden Programme Group (EHPG) meeting*.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science*, 42(4):237–270.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT press.

Leveson, N. and Thomas, J. (2013). *An STPA primer*.

Leveson, N. and Thomas, J. (2018). *STPA Handbook*.

Merriam-Webster (2018). "prioritization". Retrieved 2018−05−03. URL : https://www.merriam-webster.com/dictionary/prioritization.

Moss, T. and Woodhouse, J. (1999). Criticality analysis revisited. *Quality and reliability engineering international*, 15(2):117–121.

Norge, S. (2008). Ns 5814 krav til risikovurderinger. *Oslo: Standard. no. Hentet Februar*, 9:2016.

Oreda (2002). *Offshore reliability data handbook*. OREDA Participants.

Papic, L. and Aronov, J. (1996). A fuzzy approach to ranking procedure of systems elements according to criticality degree. *Proceedings of Advanced Manufacturing Processes, Systems and Technologies*, page 291.

Pelaez, C. E. and Bowles, J. B. (1994). Using fuzzy logic for system criticality analysis. In *Reliability and Maintainability Symposium, 1994. Proceedings., Annual*, pages 449–455. IEEE.

Rachman, A. and Ratnayake, R. C. (2015). Implementation of system-based hazard analysis on physical safety barrier: A case study in subsea hipps. In *Industrial Engineering and Engineering Management (IEEM), 2015 IEEE International Conference on*, pages 11–15. IEEE.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety science*, 27(2):183–213.

Rausand, M. (2013). *Risk assessment: theory, methods, and applications*, volume 115. John Wiley & Sons.

Reaves, C. C. (1992). *Quantitative research for the behavioral sciences*. John Wiley & Sons.

Rodríguez, M. and Díaz, I. (2016). System theory based hazard analysis applied to the process industry. *International Journal of Reliability and Safety*, 10(1):72–86.

Rokseth, B., Utne, I. B., and Vinnem, J. E. (2017). A systems approach to risk analysis of maritime operations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 231(1):53–68.

SAE (1994). Potential failure mode and effects analysis in design (design fmea), potential failure mode and effects analysis in manufacturing and assembly processes (process fmea) reference manual. *Surface Vehicle Recommended Practice, J1739*.

Song, Y. (2012). *Applying system-theoretic accident model and processes (STAMP) to hazard analysis*. PhD thesis.

SRA (2015). Sra glossary.

Thomas, J. (2017). *A Process for STPA*.

Thomas, J., Lemos, F., and Leveson, N. (2012). Evaluating the safety of digital instrumentation and control systems in nuclear power plants. *NRC Technical Researcy Report2013*.

Tjomsland, Ø. and Lie, A. H. (2017). Installation and imr on a subsea production system. Master's thesis, NTNU.

Wheeler, D. J. (2011). Problems with risk priority numbers. *Quality Digest Magazine*.

Zikrullah, N. A. (2017). Systems-theoretic process analysis (stpa) of subsea gate box system. *TPK4450 RAMS Specialization Project*.