NTNU – Trondheim
Norwegian University of
Science and Technology

Methodology for Identification of Dangerous Combinations of Output States of SIS

Yining Dong

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: July 2015
Supervisor: Yiliu Liu, IPK
Co-supervisor: Håkon Dahl-Olsen, Lloyds' Register Consulting
Mary Ann Lundteigen, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

Preface

This report is the result of master project executed Spring 2015, and is the final step in graduating as an Engineer with a MSc degree from Norwegian University of Science and Technology (NTNU). The master project is in collaboration with Lloyd's Register Consulting (LRC). LRC is affiliated to Lloyd's Register Group, and provides independent risk management and engineering dynamics services to a wide range of international clients. Reliability and Asset Performance is a part of LRC's service mainly covering reliability and SIL, data and uncertainty analysis, failure modes and effects analysis, and RAM and asset performance. The organization is committed to continuous improvement in the main business to meet customer demand.

The title of the thesis is "Methodology for Identification of Dangerous Combinations of Output States of Safety-instrumented System" and is accomplished under the supervision of Associated Professor Yiliu Liu at the Department of Production and Quality Engineering at NTNU. Co-supervisor is Senior Consultant Håkon Dahl-Olsen at LRC in Trondheim.

The thesis is on the subject of hazard identification in process industry. The potential hazard is sort of "hidden unsafe state" that should be identified during SIS design. It is assumed that the reader has some basic knowledge about process control design, preferably safety instrumented system in process industry, and is familiar with IEC61508 (2010) and IEC61511 (2003).

I would like to express my deepest and sincere gratitude to Håkon Dahl-Olsen for his guidance, understanding and encourage through my master project. His solid background in chemical engineering and process systems engineering, together with his professional experience in process safety and reliability (hardware and software requirements) provide me meaningful insight into the topic. The inspiration of this master project stems from his project experience. During regular meeting with him, I have gained new knowledge and skills in process control and optimization. Without Håkon's thoughtful and friendly approach, it would have not been possible to accomplish this report. I would also like to thank Associate Professor Yiliu Liu for providing me with practical information in report writing, and Consultant Hassan Ali at LRC in Trondheim for assisting me through case study and helping

me with practices in *OLGA* Flow Assurance.

Yining Dong

Trondheim, Norway

July 10, 2015

Summary

Many operations in process industry and other application sectors involve inherent risk due to different hazards. A safety-instrumented system (SIS) is installed to prevent development of a hazard to an accident or to reduce associated consequence. The topic of reliability assessment of SIS has been widely discussed. However, identification of dangerous combinations of output states of SIS has not been paid enough attention by industry so far. It is a requirement stating explicitly in IEC 61511 Chapter 10.3.

Normally, a SIS is designed in process system with a local perspective. The designer of SIS always analyses operational upsets in one part of the system individually, without considering the effects on system level caused by individually local effects occurring simultaneously in different parts in a large system. During process operation, such combinations of individual safe states in the SIS can cause a new situation that is dangerous. Although there are many different acceptable hazard identification methods, none of them is particularly suitable in the task of identification of the specified hazard. This report provides background and rationale for mostly common hazard identification methods. Main purpose is to propose a method, which can help to fill in the blanket of current solutions and can be applicable so that dangerous combinations of output states of SIS are able to be identified during process design and to be involved in safety requirement specification (SRS).

A three-step method is proposed based on algorithms that typically present in modular process flowsheet simulator, qualitative hazard identification method and dynamic simulation. The three steps are:

Step 1: Carry out system breakdown.

Step 2: Identify dangerous combinations of safety trips.

Step 3: Perform dynamic simulations.

The analysis is based on a critical assumption of time-scales of dynamic responses. The hazard event resulting from simultaneous trips is only considered, when a same time-scale is utilized for determining the leading effects on process or plant. A stepwise analysis guides the analyst to confirm a list of dangerous combinations of safety trips. Probability assessment is taken into account with the purpose to focus

on severe scenarios. Dynamic simulation is implemented to determine whether the combination violates the design limits of the process or plant from any starting point, where safety trips are occurring at the same time.

Nowadays, there is an increasing number of subsea-well tied in topside platform in Norwegian Continental Shell (NCS) as well as many project requiring reassessing the capacity of previously designed flare header. Evaluation of effect in flare header (on system perspective) during blowdown is indispensable, even if depressurisation system (mostly SIS) is installed to protection process unit and pipeline on local level. Dynamic modelling plays a critical role in assessment of maximum allowable operational conditions in flare line. By taking advantage of *OLGA* Dynamic Multiphase Flow Simulator, the transient process with a comparison between two different scenarios, full blowdown and blowdown (BD) with a time sequence is presented by a case study. When an existing flare header can not be replaced due to limited project budget, a proper time sequence of BDV opening is an alternative solution to avoid overcapacity of flare header. The results of the first case study reveal that evaluation regarding different combinations of tripping BDVs is necessarily executed during design of the time sequence.

In addition, the second case study is based on a process system consisting of a single piece of CSTR and cooling system. A dynamic model is established in Matlab. The case study demonstrates the applicability of the suggested three-step method, while the results of dynamic simulation confirm that simultaneously occurring safety trips can generate a hazard event. It is a valuable outcome to raise awareness to the industry about the specified hazard event. During process design, the work of identification of dangerous combinations of output states of SIS can not be disregarded.

Nomenclature

$ALARP$	As Low As Reasonably Possible
BD	Blowdown
BDV	Blowdown Valve
CCF	Common Cause Failure
$CCPS$	Centre for Chemical Process Safety
$CSTR$	Continuously Stirred-tank Reactor
$C\&E$	Cause and Effect
$E/E/PE$	Electrical/Electronic/Programmable Electronic Safety-related System
ETA	Event Tree Analysis
EUC	Equipment Under Control
$FMEA$	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
$F\&G$	Fire and Gas
$HAZID$	Hazard Identification
$HAZOP$	Hazard and Operability
$HIPPS$	High Integrity Pressure Protection System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
$LAHH$	Level Alarm High High
$LALL$	Level Alarm Low Low
$LOPA$	Layer of Protection Layers
$MTTR$	Mean Time to Restoration

$PAHH$	Pressure Alarm High High
$PALL$	Pressure Alarm Low Low
PFD	Unavailability of Failure on Demand
PFH	Average Frequency of Dangerous Failure Per Hour
PHA	Preliminary Hazard Analysis
PSD	Process Shutdown
QRA	Quantitative Risk Assessment
RAM	Reliability, Availability and Maintainability
RPN	Risk Priority Number
RRR	Rapid Risk Ranking
SAR	Safety Analysis Report
SIF	Safety-Instrumented Function
SIL	Safety Integrity Level
SIS	Safety-Instrumented System
SRS	Safety Requirement Specification
$SWIFT$	Structured What-if Technique

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

Many operations in process industry and other application sectors involve inherent risk due to different hazards. A safety-instrumented system (SIS) is installed to prevent development of a hazard to an accident or to reduce associated consequence. A SIS is generally composed of input elements (e.g. sensors, transmitters), logic solvers (programmable logic controllers, relay logic systems) and final elements (e.g. safety valves). IEC61508 [1] and IEC 61511 [2] are two important standards in process industry that provide a general frame work and requirements for the design, development and operation of a SIS[1].

It is a requirement in IEC61511 [2] that any dangerous situations caused by combination of outputs from SISs should be identified and expounded in safety requirements specification[2] (SRS). One quotation from IEC61511 [2] states that, (IEC61511-1 Chapter 10.3)

"Identification of the dangerous combinations of output states of the SIS that need to be avoided."

However, this requirement has not been fully respected by current industry, even though the industry attempts to utilize a well-adopted hazard identification technique, hazard and operability (HAZOP) study, to fulfil the requirement.

Normally, a SIS is designed in the process system with a local perspective [3]. The designer of SIS always analyses operational upsets in one part of the system individually, without considering the global effects on a system level caused by individually local effects occurring simultaneously in different parts in a large system. For some situations, such combinations of individual safe states in the SIS may

[1] These standards use the term electrical/electronic/programmable electronic (E/E/PE) safety systems as SIS.

[2] The SRS contains the relevant key information for use in specifying an operating the instrumented functions that have to be implemented by SISs. For detailed information of SRS content, reference is made to IEC61511-1, chapter 10.3 and to NOG070 annex E.

cause a new situation that is equally challenging. A continuously stirred-tank reactor (CSTR) producing liquid product is considered as an example (see Figure 1.1). It is an exothermic reaction. The reactor is devised with a cooling loop, where a cooling medium pump injects cooling stream. Two safety PSD (process shutdown) functions are installed in the system, including level alarm low low (LALL) and pressure alarm low low (PALL). If LALL is initiated, the outlet process shutdown valve (XV1) will be automatically tripped with the purpose to increase residence time in reactor. When leakage is detected in the cooling loop, PALL is on demand. Cooling medium pump will be correspondingly switched off. Considering basic design principles, two safety functions are individually safe. What if the LALL and PALL are triggered simultaneously, outlet is blocked, exothermic reaction continues with inflow of reactants, and loss of cooling system occurs at same time, the reaction will be runaway?

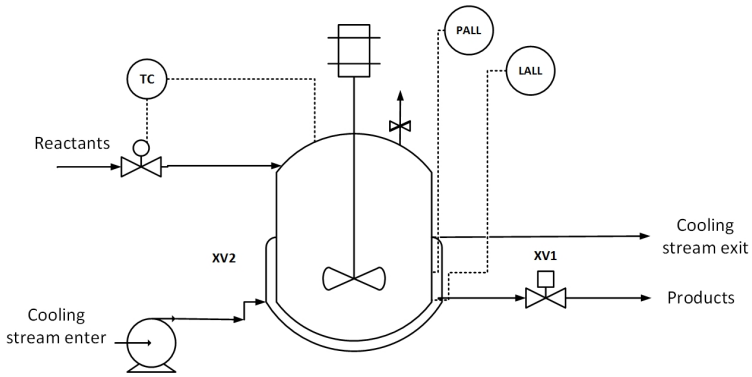

Figure. 1.1 *A sketch of CSTR producing a liquid product*

NOTE: It is notified that the purpose of presenting this example is to reveal the problem in terms of SIS design. The property and composition of the reaction are not described in detail.

Today it seems evident that, at least in Europe, IEC61511 [2] becomes a central standard for specification, design and operation of SIS in process industry [4]. In Norway, the offshore Oil & Gas industry is one major area for the use of IEC61511 [5]. IEC61511 [2] requires identifying such hazards stemming from simultaneous activation of safety trips. It has become customary in current industrial practice to refer to hazard and operability (HAZOP) studies as proof that such output combinations do not exit. Unfortunately, HAZOP is not a favourable solution due to inherent limitations.

1.2 HAZOP Study and Limitations

A Hazard and Operability (HAZOP) study[3] is a structured and systemic examination of planned or existing process or operation with the purpose to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation [6]. It is usually performed by a multidisciplinary team (HAZOP team) in a series of meetings. HAZOP approach was initially developed to be used during the design phase, but can also be applied to systems in operation. The most common HAZOP study is accomplished during the detailed engineering phase.

In HAZOP study, the system or plant is divided into a number of study nodes. The study nodes are examined one by one. For each node, design purpose and the normal state are defined. A set of guidewords and process parameters (see in Chapter 3) are used to facilitate brainstorming of possible deviations in the system. The brainstorming is normally led by a set of HAZOP questions. For instance, the guideword can be "High" and the process parameter is "Pressure". Thus, the HAZOP question could be raised as "could there be high pressure", "if so, how could it rise" and "what are the consequences of high pressure". Safeguards intend to reduce frequency of occurrence and/or mitigate the consequences. As seen from Table 1.1, the worksheet depicts the results of a HAZOP study.

Table. 1.1 *HAZOP study results [2]*

Item	Deviations	Causes	Consequences	Safeguards	Actions
Vessel	High flow	Flow control loop fails	High flow leads to high pressure		
	High pressure	Flow control loop fails; External fire	Vessel damage and release to environment	High pressure alarm; Deluge system; Pressure relief valve	Evaluation design conditions for pressure relief valve release to environment
	Low/no flow	Flow control loop fails	No consequence of interest		
	Reverse flow		No consequence of interest		

[3]The term HAZOP has been often associated in generic sense, with some other hazard identification techniques (e.g. checklist HAZOP, HAZOP 1 or 2, knowledge-based HAZOP). The use of the term with such techniques is considered to be inappropriate and is specifically excluded from this document.

NOTE: For this example, it is assumed that the vessel can experience high pressure due to the inability of the down stream equipment to handle full gas flow from the vessel when the feed flow is too high.

Besides HAZOP study, there are other types of tools and techniques available for the identification of potential hazard and operability problems as well, such as Checklists, Fault Modes and Effects (FMEA) and Fault Tree Analysis (FTA). Some techniques, such as Checklists and What-if analysis, can be used early in the system lifecycle when little information is available, or in later phases if a less detailed analysis is needed. Compare with those methods, HAZOP studies require more details regarding the systems under consideration, but produce more comprehensive information on hazards and errors in the system design.

Whilst HAZOP studies have proved to be extremely useful in diverse industries, the technique has limitations that should be taken into account when considering a potential application [7]. First of all, HAZOP study considers system parts individually and methodically examines the effect of deviations on each part. As such, it may not be able to identify hazard related to interactions between different nodes. Many systems are highly inter-linked, and a deviation at one of them may have a cause elsewhere. Adequate local mitigating action may not address the real cause and still result in a subsequent accident. Another drawback is that HAZOP study is strongly dependent on the facilitation of the leader and the knowledge of HAZOP team. Last but not least, conventional HAZOP study is typically optimized for process hazard so that plant-wide[4] effects may not be efficiently uncovered. In particular, events following a global system shutdown are not discussed in a HAZOP study, such as release of blowdown due to fire or confirmed gas detection on an offshore production. These limitations may explain why a HAZOP team most likely fails to identify effects from simultaneously occurring initiated events. For further information about the methodology as well as limitations of HAZOP study, there are two books [6] [9] and one standard [7] that can be referred to.

Furthermore, purely qualitative studies like HAZOP are typically efficient for steady-state effects and simple dynamic effects, whereas the hazard specified in current master project would predominantly be a transient process. As the pitfalls of a HAZOP study, it emphasizes the need of a methodology for hazard identification that can identify dangerous output combinations from SIS. Dynamic simulations plays a critical role to capture the transient process.

[4]The terms of process and plant are almost synonymous terms in the control community. A process usually refers to the 'process itself' (without any control system) whereas a plant may be any system to be controlled (including a partially controlled process). However, not that in the chemical engineering community the term plant has a somewhat different meaning, namely as the whole factory, which consists of many process units; the term plant-wide control is derived from this meaning of the word plant [8].

1.3 Ideas of a Methodology Based on Dynamic Simulation

Both modelling and software technology for a dynamic simulation are much more demanding, compared to steady-state simulation [10]. Prior to performing dynamic simulation, it is necessary to prepare a list of scenarios through a series of analyses. In process control design, it is always challenging to estimate how long it takes a technical system to respond when input changes, or how much an output variable will change in response to one or more inputs [8]. What engineers are skilled in, however, is to identify the direction of change itself as well as the order of magnitude of change. It is possible to take advantage of the experience from skilled people to brainstorm potential scenarios. This indicates that it should be possible to use a type of qualitative screening of scenarios based on people's experience. HAZOP technique mentioned above is an attempt to apply engineering experience to weed out problems at the design stage, as well as during modification work in operations. However, experience may be deficient and inferior in the case if new hazards is generated due to trips arising at the same time.

A large technical system has many safety functions, which is true not only for an oil and gas platform but also for a train or an automobile using as transportation in daily life. There could be more than five hundred such safety functions in a whole oil and gas platform [11]. If all possible combinations of trips transpiring simultaneously are considered, 10^{150} combinations have to be checked. The number is much larger than the total number of molecules in the entire universe. If a supercomputer would use millisecond to analyse such a combination, the whole operation would take significantly longer time than the age of the universe.

The comforting fact behind the crucial scene is that most trip combinations hardly lead to undesired consequences because the extremely weak connections and the retardation effect between them seldom affect local performance [12]. In fact, this will be the case for almost all such trips. In addition, many trips are unlikely to create new dangerous situations. The number of scenarios is conceivably restricted with accordance to people's experience. Thus, one part of the work prior to dynamic simulation is to exclude pairs of trips that have little influence to do with each other.

1.4 Objective

The main objective of this master thesis is to establish a generic methodology that can be applied to identify the dangerous (global) states, when several individual safe (local) states occur concurrently. To deal with this practical issue in SIS design and verification, the following specific objectives are considered.

1. Explain the potential safety issue due to individual safe states occur concurrently in the system.

2. Perform a literature review in terms of hazard identification methods, which are commonly used in process industry. Discuss the limitations of current solutions for identifying the specified hazard.
3. Give a thorough presentation of the proposed methodology that can be generally applied to identify the dangerous combination of output states of SIS. The methodology shall be stepwise with a clear description of each step.
4. Apply case studies to demonstrate the applicability of proposed methodology. Summarize the main outcomes from case studies.
5. Identify and describe topics within the framework of this project that need further research.

1.5 Limitations

The master project is executed in a limited time frame, constraining the coverage of the topic. The coverage is also restricted by author's limited knowledge in the field of process control engineering as well as a little professional experience in risk analysis. Dynamic models establishing in case studies are lack of actual project data. Since the method is tested with a simple process system, the applicability of the method for a complex process system requires further discussion. The reader should have basic understanding of process control design and HAZOP study. In addition, knowledge of IEC61508 [1] and IEC61511 [2] is an advantage.

1.6 Structures

The report is organized as follows:

- Chapter 1 provides a problem description of identification of dangerous outputs combination of SIS during process or plant design phase. Based on a short presentation of HAZOP study, the limitations of the method are discussed. General ideas of a methodology based on dynamic simulation is presented.
- In Chapter 2, a general overview of SIS and its design requirements are given. Potential hazardous events due to simultaneously occurring safety trips are further identified and described. With regard to a potential safety issue due to local perspective in SIS design, the consideration of global effect from a system prospective is suggested. Design of blowdown and flare header system in offshore platform is briefly introduced as a typical example to present the essential of hazard analysis from a system point of view.
- Chapter 3 provides a short presentation of IEC61511 [2] and safety lifecycle. A literature review is performed in terms of different hazard identification

methods using in process industry. Moreover, LOPA as a representative of SIL determination method is simply introduced, and interface between HAZOP and LOPA worksheet is discussed.

- In Chapter 4, a three-step method is developed based on algorithms in the field of modular process flowsheet simulator, methodologies in hazard identification and dynamic simulation.
- Chapter 5 describes a suggested work procedure for probability assessment of the hazardous event.
- Chapter 6 provides a case study of flow network with multiple releases to flare header. A general overview of dynamic simulation of flare header, flare system on topside platform and *OLGA* Flow Assurance software is given.
- In Chapter 7, the applicability of the proposed methodology in Chapter 4 is evaluated in a case study of process system consisting a CSTR and cooling system. The basic theories including mole balance and energy balance for establishing dynamic model are introduced.
- Chapter 8 presents conclusion, discussion and suggestions to future work.

2 Dangerous Combinations of Output States of SIS

2.1 Safety Instrumented System

Rausand and Høyland (2004) [13] describe a SIS as a system comprising sensor(s), logic solver(s) and final element(s), and can be looked upon as an independent protection shell for machinery or equipment. What the system shall protect is referred to as equipment under control (EUC) and is defined as *"Equipment, machinery, apparatus, or plant used for manufacturing, process, transport, medical, or other activities"* [1]. A SIS[1] implements the wanted safety function needed to maintain a safe state of the equipment and has the function of achieving the essential risk reduction given by the requirements [1].

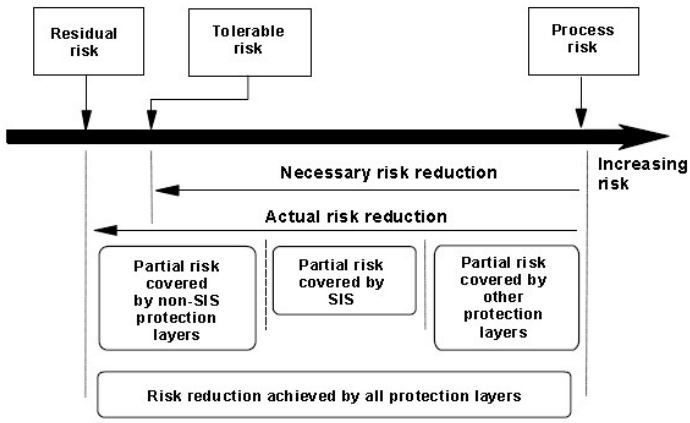

Figure. 2.1 *General concepts of risk reduction [2]*

[1] A SIS may implement one or more safety-instrumented functions (SIFs).

Figure 2.1 describes general concepts of risk reduction in process industry. Based on the risk calculated for the equipment under control (EUC), a decision should be made on whether a SIS is required to achieve the desired functional safety. During risk evaluation, priority is always given to the elimination of a hazard as source, if possible. Otherwise, one or more SISs and/or other risk reduction measures need to be implemented to achieve a tolerable risk. There are requirements in terms of both safety function and safety integrity for a safety-instrumented function (SIF). Thus, to maintain the desired risk reduction, these two requirements shall be fulfilled. The safety function requirements for an SIF imply two aspects: First, it should perform the intended (redefined) function when a process demand occurs within a reasonable period of time. Second, it should not be activated without a process demand from the EUC with respect to the hazardous event under consideration.

Safety integrity requirements can further be classified as qualitative, semi-quantitative and quantitative. Qualitative requirements are mainly concerned with techniques and measures that should be implemented to avoid and control both hardware and software systematic failures. Semi-quantitative requirements are related to the behaviour of components, and are expressed in terms of architectural constraints. Quantitative requirements measure the probability that an SIF satisfactorily performs specified safety functions under all the stated conditions within a stated period of time. Safety integrity level (SIL) is classified into four levels, SIL 1, SIL 2, SIL 3 and SIL 4, with SIL 4 being the most reliable and SIL 1 being the least reliable [1]. In Table 2.1, the PFD related to the four SILs for low demand of operation is presented. The PFD is the average safety unavailability of an item, thus the mean proportion of time the item does not function as a safety barrier.

Table. 2.1 *SIL for safety functions operating in low demand of operation [2]*

Safety integrity level (SIL)	**Average probability of failure to perform its design function on demand**
4	$\leq 10^{-5}$ to $< 10^{-4}$
3	$\leq 10^{-4}$ to $< 10^{-3}$
2	$\leq 10^{-3}$ to $< 10^{-2}$
1	$\leq 10^{-2}$ to $< 10^{-1}$

When SIS is considered as a critical safety barrier in process industry, much effort has been made in terms of unavailability quantification of safety system. Rausand M. wrote a book [14], which particularly concentrates on quantitative reliability analysis of the hardware of E/E/PE safety related systems. Besides the methods and formulas suggested in IEC standards (i.e. IEC61508 [1]), there are currently many optional methods [15] and formulas [16] with respect to reliability assessment of safety-critical systems. However, the use of SIS can also bring challenges to process industry in spite of the reliability of instrumented system from product

development perspective. When SIS is implemented in a process or plant, it may get rise to potential safety issues, which has not been uncovered or not been paid enough attention.

2.2 Hazard Events Due to Simultaneously Occurring Safety Trips

Kletz [17] attempts to highlight a fact that sometimes other risks are increased in striving to make specific industrial risks ALARP (the risk should be As Low As Reasonably Possible) based on a number of real issues emerging in varieties of industries. Even though ALARP has served us well for a long time, the time has come to move on and supplement it by considering also the net safety benefits or detriment. In addition, Etchells wrote an article [18] to discuss safety benefits and pitfalls of process intensification. Based on the opinions of these two authors, it induces a concern of potential safety issues, as SIS is considered as a essential risk mitigation measure in process or plant.

Hazard is an inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment [19]. A basic understanding of hazard and the potential for hazard events is essential for persons involved in hazard and risk analysis. Some hazards are particularly considered in chemical and petroleum industry, involving exploration, fire, toxic materials release, mechanical failures and wrong chemistry (creating the wrong substance through malfunction of the process). Fire and gas detection system, process shutdown systems and emergency shutdown systems are examples of SISs used to prevent abnormal operating conditions from developing into an accident. Such systems are thus installed to reduce process risk associated with health and safety effects, environmental impacts, loss of property, and business interruption costs.

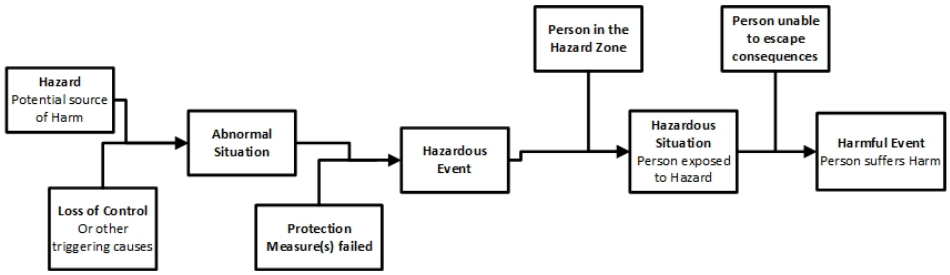

Figure. 2.2 *Harmful Event [2]*

In accordance to IEC61511 [2], a sequence that describes how hazard leads to harmful event is demonstrated in Figure 2.2. It shows how loss of control or any other causes result in an abnormal situation and place a demand on protective

measures, such as safety alarms, SIS, relief valves etc. A hazardous event takes place when a demand occurs and the relevant protective measures are in a failed sate, and do not function as intended.

A SIF is a function that has been intentionally designed in order to protect the EUC against demand. The interactions of SIFs may generate a potential hazard event, if the SIFs are often specified for a process deviation. There can be a situation that protection measure(s) does not fail to react the abnormal situation, however, a new hazardous event is caused by simultaneously occurring safety trips. Without a comprehensive analysis, it has the possibility to become an accident, which is harm to human life, economic assets and environment. In agreement with the concern, the sequence how hazard leads to a hazard event is modified and is redrew in Figure 2.3. The new drawing indicates a hazard event can be generated due to simultaneously occurring safety trips, when several SIFs are activated to avoid the occurrence of a specific hazardous event. In order to achieve an acceptable risk level, it is necessary to identify this type of hazard during process design.

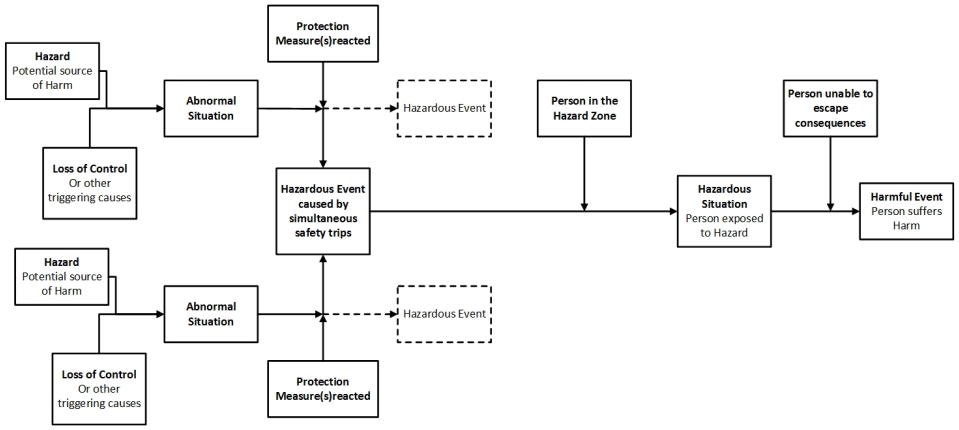

Figure. 2.3 *Hazard event caused by simultaneously occurring safety functions*

Note: The sources of harm do not have to be different types. The situation can be derived from a same type of source but it induces several safety trips at the same time. The harmful event can also be harm to material asset and environment instead of human life.

2.3 SIS Design in Process with Consideration of Global Effects

A chemical process is a series of interconnected units. For instance, most of process consists of a reaction section and reactor effluent, which is a mixture of products and

unreacted materials. In order to obtain the desired product, the reactor effluent would be taken to as a separation section, where the unreacted materials will be separated from the products. The key point is that unreacted materials are always recycled back to reaction section essentially due to economic consideration. Sometimes, it may be also considered as environmental-friendly design.

Material and energy recycles are typical in chemical processes. Also, manipulating a process stream disturbs the connected units, while the recycle may propagate the variability through the entire plant. A simple illustration is a distillation column connected to a continuous stirred-tank reactor (CSTR) (shown in Figure 2.4).

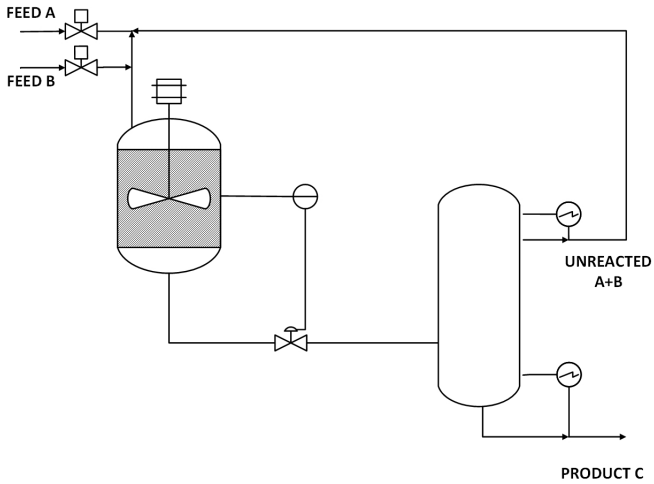

Figure. 2.4 *Illustration of a distillation column connected to a CSTR*

The process is to put in fresh A and fresh B, while A reacts B to give C in reactor. The reaction doe not go completion in the reactor so that the affluent from the reactor is a mixture of A, B and C. This mixture is sent to a distillation column, where C being heavy comes down the bottoms of distillation column and unreacted A & B come to the top. Due to economic consideration, A and B are recycled back to the reactor. The point is that the reactor level should be controlled tightly because residence time in the reactor affects the conversion. In order to hold the conversion constant, it needs to hold the level inside the CSTR constant by using a level controller. As adjustment, the flow is not transformed to the distillation column as the variability in the level in CSTR.

Because of the interactions, the distillation column is disturbed in order to hold the level constant in CSTR. Since the distillation column is feeding back to the reactor with the unreacted materials, it in return influences the reactor, when it attempts to hold the level constant in distillation column. In chemical process, recycle loop may propagate the variability through the entire plant. Holding the reactor level constant may cause variability to go through and oscillate the entire plant.

It is same for implementation of SIS. For instance, a PSD function, i.e. pressure alarm high high (PAHH), is installed in CSTR. When PAHH is initiated, the safety function is supposed to close one critical valve, i.e. a process shutdown valve located in inlet line to CSTR. In order to protect the pressure inside of CSTR, the inflow of materials is stopped. Based on the example of CSTR connected with a distillation column, stopping inflow of materials will disturb the connected unit of CSTR, such as a distillation column. Because of the recycle loop, the variability goes through and oscillates entire plant if a safety trip, i.e. level alarm high high (LAHH) in distillation column occurs simultaneously.

However, SIS is often designed in a system with a local perspective (refer to Section 1.1). As shown in Figure 2.5 (left), it presents how standard safety functions are designed in attempts to protect a single process unit or a part of plant. For instance, a PAHH is installed in CSTR as a safety barrier to avoid the occurrence of hazardous events (e.g. fire or exploration), occurring in CSTR. From a process design perspective, the approach is improper because the effect of local safety trips on (global) system level is not evaluated. It is unrealized or disregarded that a safe function (i.e. PAHH stops the material flow) generates disturbance to the connected units as the nature of process operation. In addition, the variability goes through entire plant via recycled loops. In Figure 2.5 (right), the model reveals a systematic method of designing safe functions for a (chemical) plant. The big rectangular represents a plant, while blocks numbering with 1 and 2 denote two equipment in the plant. The effect of local safety trips on (global) system level and interactions between process units are emphasized by using arrows and lines, respectively. For instance, the effect on system level is necessarily assessed, when a PSD function is initiated in equipment 1. Designers should carry out a comprehensive analysis, if a safety function is considered in a local system.

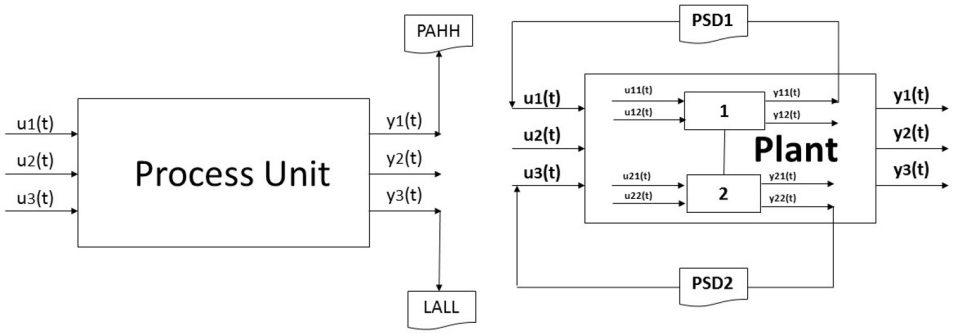

Figure. 2.5 *A new concept of SIS design (Left: SIS is designed in process with a local perspective. Right: SIS design with consideration of global effect)*

If several safety functions, i.e. PSD functions, in a process or plant is on demand at the same time, the complexity of the case is correspondingly increased. As the example of CSTR described in Section 1.1, it can be dangerous when two safety

functions are initiated simultaneously in different parts of system. Like runaway reaction with loss of cooling, the result can be a disaster. Therefore, dangerous combinations of output states should be precisely identified in the early stage of process design to avoid potential risk. In order to evaluate the actual effect of a considerable combination of output states of SIS, it needs to explore the transient process, how the output variables change over the time. Dynamic simulation can be used in the analysis.

So far, there are few resources in both academia and industry concerning the safety issues due to simultaneous occurring safety functions in process industry. As the SIS is widely installed in process industry including offshore Oil & Gas industry, it is necessary to raise awareness of whole process design team and risk analysts with respect to global effect on system level during SIS design and verification.

2.4 Design of Blowdown and Flare System

Depressurisation is one of key parameters relevant for the fire protection of process system [20]. The primary mean of protection is that blowdown (depressurisation) is supposed to be as fast as possible. Blowdown (BD) times is normally in accordance to specified requirements for protection of pressurised systems exposed to fire. Evaluations regarding material capacity versus BD can be performed as specified in "Guidelines for protection of pressurised systems exposed to fire" by Scandpower Risk Management AS[2] or similar method. Depressurisation may be performed for a process segment, a fire area and the entire plant[3] .

All pressure vessels and piping segments, which during shut down contain more than 1000 kg of hydrocarbons (liquid and/or gaseous), shall be equipped with a depressurising system [21]. In the design of offshore oil and gas platform, a blowdown (BD) and flare (vent) system plays a critical role in terms of depressurisation. Activation of BD shall be automatically initiated upon confirmed fire detection in hazardous area. Sufficient time for sectionalisation valves to close shall be allowed before opening of BDVs. Moreover, the design of flare header capacity should guarantee the safety during a full platform blowdown.

In the recent years, the number of subsea tie-in project is dramatically increasing in the Norwegian North Sea. While it is essentially driven by the economic profit [22], some potential safety issue also emerges. Many efforts have been done on the local system level in order to protect the process units including pipelines, such as HIPPS (high-integrity pressure protection system). On the other hand, the attention is

[2]Since the company has been merged by a British company, the name of the company now is called Lloyds Register Consulting (see Preface).

[3]For some types of process demands that have a potential for a major accident, i.e. fires, gas leaks, and loss of main power, the ESD system is activated. The required ESD actions are usually grouped into several levels, depending on the type of deviation/demand that is detected and where it is detected. One reference of ESD principle hierarchy is given to NORSOK S-001 Section 10.4 [21]. NOSOK S-001 is a national standard in terms of technical safety.

also paid to the evaluation of safety facilities from a (global) system point of view. For instance, there is a reassessment of flare header on topside, when the number of production wells is increased. With respect to a safety concern, the flare header may need to be replaced by a new one, if the situation of a full blowdown exceeds the original design limits. However, the cost is perhaps too high to invest on installation of a brand new flare header. Then, an alternative is to design a time sequence of blowdown initiations. In order to create a proper time sequence, it is essential to investigate different combinations of output states of BD system.

Modification of BD system in subsea project exposes the importance of evaluating the global effect, even if the safe design is accomplished on the local system level. In order to see the transient processes in flare header with different BDVs opening scenarios, a case study is presented in Chapter 6. The model is simulated in a commercial dynamic simulation software, *OLGA* Flow Assurance. More information of blowdown and flare system as well as *OLGA* software is described in Chapter 6.

3 Hazard Identification in Development of SIL Requirement

3.1 Introduction to IEC61511 and Safety Lifecycle

Today it seems evident that, at least in Europe, IEC61508 [1] is the central standard for specification, design and operation of safety instrumented systems (SIS) [23]. Hence, the standard has a major impact on the safety work e.g., within the process industry. Whereas IEC61508 [1] is a generic standard common to several industries, the process industry is currently developing its own sector specific standard for application of SIS, i.e. IEC61511.

IEC61511 [2] is the main standard for the application of safety-instrumented systems (SISs) in the process industry. The standard consists of three parts, under the general title *Functional safety: Safety Instrumented Systems for the Process Industry Sector:*

Part 1: General framework, definitions, system, hardware & software requirements;

Part 2: Guidelines for the application of Part 1;

Part 3: Guidelines for the determination of the required safety integrity level.

IEC61511 [2] applies when a SIS is based on proven technology or technology whose design has been verified against the requirements in IEC 61508 [1]. Development of new technology is beyond the scope of IEC 61511 [2]. For this reason, IEC 61511 [2] is sometimes called the end-user's and system integrator's standard, whereas IEC61508 [1] is called the manufacturer's standard.

The safety lifecycle is an important concept in IEC61508 [1] and its sector-specific standards including IEC61511 [2]. Both IEC61508 [1] and IEC61511 [2] use the "safety lifecycle" as a framework in order to structure overall technical and nontechnical requirements relating to specification, design, integration, operation, maintenance, modification and decommissioning of a SIS. The safety lifecycle presented in IEC61511 [2] can been seen in Figure 3.1.

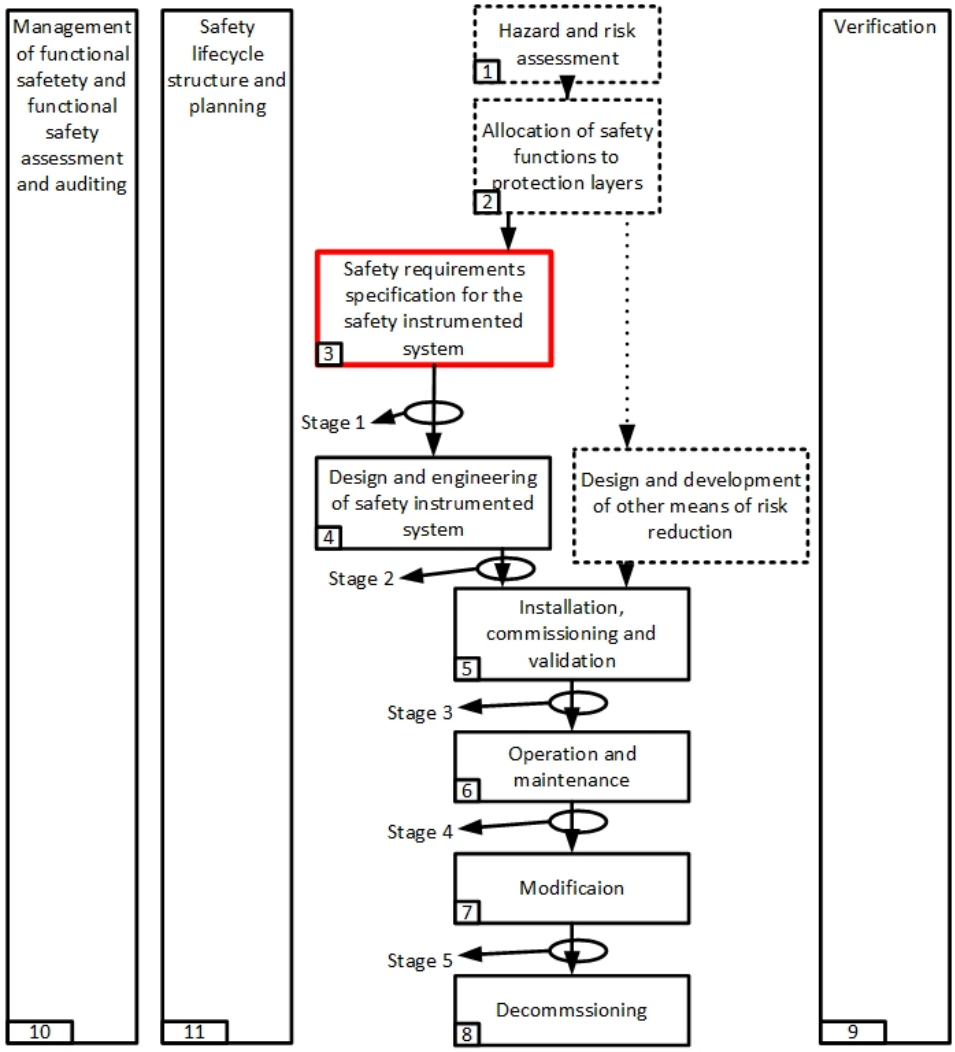

Figure. 3.1 *Safety lifecycle model in IEC61511[2]*

The foundation for any safety system application is a thorough understanding of the problems to be solved [19]. The starting point for an SIS is the safety requirement specification (SRS), which is red box in Figure 3.1. Regarding the input requirements for developing SRS, much of the information stems from a good knowledge of the manufacturing process, its normal operations, and its potential hazards. During the hazard and risk assessment, it is to identify the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event as well as the process risks associated with the hazardous event. Based on estimated process risk, the objective is to determine

any requirements for risk reduction and the safety functions required to achieve the necessary risk reduction. The outcome of hazard and risk assessment determines if any of the safety functions are SIFs, which are implemented by SIS. During the activity of allocation of safety functions to protection layers, the SIL is determined. LOPA may be applied during this phase, but other methods like risk graph and safety layer matrix are also applicable.

As clarified in Chapter 1, the objective of this master project is to involve identification of dangerous combination of output states of SIS in SRS. "Hazard and risk assessment" and "allocation of safety functions to protection layers" are the most interesting, since those two phases give the input to SRS. According to [1] [13], all of these activates are executed in the design prior to final design and manufacturing.

3.2 Hazard Identification Methods

There are not so much descriptions regarding hazard identification methods in IEC61511 [2], while several qualitative techniques for hazard analysis are recommend in Part 3 of the standard, including safety review, checklists, what if analysis, HAZOP studies, failure mode and effects analysis (FMEA), and cause-consequence analysis. Besides them, couples of hazard identification methods are also mentioned in [6], such as hazard log and change analysis.

3.2.1 Checklist Methods

A hazard checklist is a written list of hazards or hazardous events that have been derived from past experience. The entries of the list are often formulated as questions that are intended to help the study team consider all aspects of safety related to a study object. In many cases, it is useful to start with a list of generic hazards and/or generic hazardous events and to decide if, where, and how these events may occur for the system being analysed. An example of process/system checklist during design phase is presented in Table 3.1. The checklist approach ensures that common and more obvious problem are not overlooked. While, it is limited to previous experience. A limitation is that hazard that have not been seen previously, can been missed.

Table. 3.1 *Process/system checklist of the design phase [9]*

Materials. Review the characteristics of all process materials: raw materials, catalysts, intermediate products, and final products. Obtain detailed data on these materials, such as:	
Flammability - What is the auto ignition temperature? - What is the flash point? - How can a fire be extinguished? **Explosively** - What are the upper and lower explosive limits? - Does the material decompose explosively? **Toxicity** - What are the breathing exposure limits (e.g. threshold limit values, immediate dangerous to life and health)? - What personal protective equipment is needed? **Corrosively and compatibility** - Is the material strongly acidic or basic? - Are special materials required to contain it? - What personal protective equipment is needed?	**Waste disposed** - Can gases be released directly to be atmosphere? - Can liquids be released directly to water? - Is a supply of inert gas available for purging equipment? **Storage** - Will any spill be contained? - Is this material stable in storage? - Static electricity - Is bonding or grounding of equipment needed? - What is the conductivity of the materials, and how likely are they to accumulate static? - What is the conductivity of the materials, and how likely are they to accumulate static? **Reactivity** - Critical temperature for auto reaction? - Reactivity with other components including intermediated? - Effect of impurities?

3.2.2 What-if Method

In the literature [6], what if method is also called structured what-if technique (SWIFT). Similar with checklist method, SWIFT is usually applied during brainstorming session where a group of experts with detailed knowledge about the study object raise generic questions to identify possible hazardous events, their causes, consequences, and existing barriers. Suggestions of alternatives for risk reduction is also given in the discussion. The result of analysis is always formulated in a worksheet. In Table 3.2, it is an example of a SWIFT worksheet. The example considers LNG (liquefied natural gas) transport by tank truck. Fre. and Sev. is the frequency and severity of each hazardous event, while RPN stands for the risk priority number of a deviation. More detailed information of the method can be referred to [6].

A SWFIT analysis is suitable for mainly the same application as a HAZOP study. Compared with HAZOP study, a SWIFT analysis usually has less focus on operability problems. It is primarily dependent on how detailed the analysis must be whether a SWIFT or a HAZOP study should be conducted. A key advantage of SWIFT is the approach is very flexible, and applicable to any type of installation, operation, or process, at any stage of the lifecycle. But it is highly dependent on checklists prepared in advance.

NO.	What if ?	Possible causes	Possible consequences	Existing barriers	Risk			Proposed improvements	Comment
					Fre.	Sev.	RPN		
1	The driver leaves without disconnecting the flexible hose?	-Time pressure -Diver distraction	-The hose breaks -Gas is released -Fire/explosion likely	Procedure	3	3	6	Install barrier in front of truck that can be opened only when the flexible pipe is disconnected	
2	The quick-release coupling of the hose is released during filling?	-Not properly connected -Technical failure in coupling	-Driver is hit -Gas is released -Fire /exploration likely	Preventive maintenance of coupling	3	2	5	-New/better coupling -Improved maintenance -Improved driver training	
3	The tank truck runs off the road on "Main Street"		-Puncture of tank (inner/outer) -Fire/exploration likely -High number of victims	-Driver training -Traffic control	2	4	6	-Improved driver training -Alternative route	

Figure. 3.2 *SWIFT worksheet [6]*

3.2.3 Hazard and Operability Study

A concise introduction of Hazard and Operability (HAZOP) study is given in Chapter 1. Here, it is to enrich the information of method by focusing on different applications of HAZOP and development of method. The HAZOP approach was developed initially to used during the design phase, but can also be applied to systems in operation. Several variants of the original HAZOP approach have been developed, such as process HAZOP, human HAZOP, human HAZOP, procedure HAZOP and software HAZOP.

The HAZOP analysis is performed in a series of meeting that are arranged as brainstorming sessions supported by guidewords, process parameters, and various checklists. A main step in the analysis is that the system or plant is should be

divided into a number of study nodes. Each study node is examined separately, when the design intent and normally state are defined. Then guidewords and process parameters are used to give rise to proposals for possible deviations in the system. The guidewords and process parameters are supposed to stimulate individual through and induce group discussion. A list of generic HAZOP guidewords is presented in Table 3.2. Moreover, typical process parameters for a chemical process are flow, pressure, temperature, level and composition. The example of HAZOP worksheet is presented in Table 1.1 in Chapter 1.

Table. 3.2 *Generic HAZOP guidewords [6]*

Guideword	**Deviation**
No/None	No part of the design intention is achieved (e.g., no flow, no pressure, when there should be).
More of	An increased above the design intention is present, more of a physical property than there should be (e.g., higher flow, higher pressure, higher temperature).
Less of	A decrease below the design intention is present, less of a relevant physical property than there should be (e.g., lower flow, lower pressure, lower temperature).
As well as	The design intent is achieved, but something else is present.
Part of	Only some of the design intention is achieved, wrong composition of process fluid. A component may be missing or of too low/high ratio.
Reverse	The design intention is the opposite of what happens.
Other than	The design intention is substituted by something different.
Early	Something happens earlier in time than expected.
Late	Something happens later in time than expected.
Before	Relating to the sequence of order, something happens before it is expected.
After	Relating to a sequence of order, something happens after it is expected.

Currently, many researchers [24]-[25] are active in the research area of combing HAZOP with dynamic simulation. The main idea is principally to determine risk from operational disturbances, and to develop means for effective risk reduction

[26]. Ramzan et al. [27] introduced a systematic methodology, supported by dynamic simulation and conventional HAZOP, for discovering operational failures and analysing the effects of design improvements in a safety system. Whereas conventional HAZOP covers both safety and operational failures, dynamic simulations guide safety teams towards generating optimization proposal for a system. Since most new methods are developed on the basis of conventional HAZOP, they may not able to serve the purpose to identify if a system has the potential to generate a new hazard when several individually safe states occur simultaneously in the process system. Nevertheless, the achievements from previous research works affirm that combining process simulation features with hazard identification techniques delivers invaluable results for safety examinations.

3.2.4 Failure Modes and Effects Analysis

The failure modes and effects analyses (FMEA) is used mainly in the design phase of a technical system to identify and analyse potential failures. It has been used to identify the possible failures of a SIF [14]. The analysis is carried out by reviewing as possible to identify failure modes, causes, and effects of such failures. For each component, the failure modes and their resulting effects on the rest of the system are entered into a specific FMEA worksheet. The analysis is qualitative, but may have some quantitative elements, including specifying the failure rate of the failure rate of the failure modes and a ranking of the severity. An sample of an FMEA work sheet is given in Appendix C. FMEA is mainly an effective technique for reliability engineering, while it is often used in risk analysis. The approach provides a comprehensive hazard ware review and is suitable for complex system. Moreover, FMEA is systematic and comprehensive, and should be able to identify all failure modes with an electrical or mechanical basis. On the other hand, a weakness of the method is that it considers hazard arising from single-point failures and will normally fail to identify hazard caused by combinations of failures.

3.2.5 Cause and Consequence Analysis

Cause and consequence analysis is similar to event tree analysis, but has another graphical layout. It integrates fault tree analysis with event tree sequence analysis, and can also combine event sequence to give a more compact tree structure. A simple illustration of a cause-consequence analysis is given in Figure 3.3.

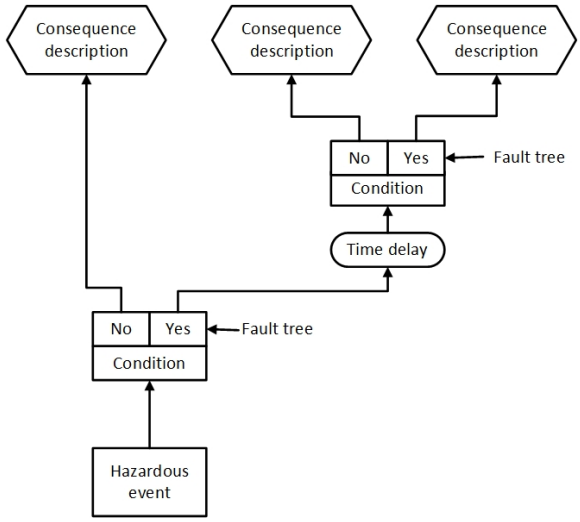

Figure. 3.3 *Cause-consequence analysis diagram [6]*

3.2.6 Other Hazard Identification Methods

Preliminary Hazard Analysis

Preliminary hazard analysis (PHA) is used to identify hazards and potential accidents in the early stages of system design, and is basically a review of where energy or hazardous materials can be released in an uncontrolled manner. A PHA is called ”preliminary” because it is usually refined through additional and more thorough studies. Many variants of PHA have been developed and they appear under different names, such as hazard identification (HAZID) and rapid risk ranking (RRR). PHA can be used in early project phases, that is, early enough to allow design changes. It is a versatile method that can cover arrange of problems. However, it is difficult to use represent events with widely varying consequence and fails to assess risks of combined hazards or coexisting system failure modes.

Hazard Log

The hazard log is also called a hazard register or a risk register. All kinds hazards that threaten a system's success in achieving its safety objectives should be logged. The hazard log is established early in the design phase of a system or at the beginning of a project and be kept up to date as a living document throughout the lifecycle of the system or project. It should be updated when new hazards are discovered, when there are change to identified hazards, or when new accident data become available. Main elements of a hazard log include hazards, hazardous

events, incidents, threats and vulnerabilities, and journal. A simple hazard log is demonstrated in Table 3.3.

Table. 3.3 *Simple HAZOP log*

System: Reference:			Name: Date created:	
Hazard/threat	**Where**	**Amount**	**Safeguard**	**Comments**
Trichloroethyylene	Storage 2	1 barrel	Locked room	
Pressurized gas	Pressure vessel 3	5 bar	Fenced	

Change Analysis

Change analysis is used to determine the potential effects of some proposed modification to as system or a process. The analysis is accomplished by comparing the new system with a know system or process. A change is often the source of deviation in the system operation and may lead to process disturbances and accidents. It is therefore important that the possible effects of changes be identified and that necessary precautions be taken.

3.3 Findings from Literature Review of Hazard Identification Methods

There are a number of methods that can be adopted in hazard analysis. Diverse techniques have different routines in analysis. For instance, FMEA focuses on failure modes, such as valve fails to close on demand, leakage through the valve or too high frication in actuator. Those are mechanical failures, which may affect the reliability of a system. On the other hand, HAZOP study starts from ”no flow” ”high temperature” or ”high temperature”, which are typical process deviations.

Each hazard identification approach has own advantages and limitations for various applications. Some hazard identification methods have been used with great success in industries. For instance, HAZOP study reviewing the process design contributes to safer, more efficient, and more reliable plant. Nonetheless, most hazard identification methods have several common limitations.

1. The analysis is dependent on the knowledge and experience of analyst.
2. It can be time-consuming and produces a lengthy documentation for complete recording.

3. The study is always based on single part of system or plant. For instance, FMEA considers hazards arising from single-point failures. It means it will normally fail to identify hazards caused by combinations of failures. Likewise, HAZOP study does not identify hazards related to interactions between different study nodes.

4. Some hazard identification approaches, such as FMEA and HAZOP study require detailed design drawing, such as P&ID drawing, which cannot be available in beginning of design phase. This brings challenges to hazard identification. In a project of offshore semi submersible rig, HAZOP studies are usually carried out in both design and construction phase. However, the changes made after construction often significantly increases overall system cost. It would be efficient to apply different techniques to identify all possible hazards in the design phase of system, when less costly changes can be made.

Moreover, some methods such as such as checklists and what-if analysis, are particularly used in the early stage in the system lifecycle when little information is available. It can be interesting to study the topic that different hazard identification methods may be suitable for specific stages in terms of project development. The Figure 3.4 shows a six-stage life cycle diagram for process hazard analysis, which is found in [19]. Along the development of a project, it outlines a six-stage hazard analyses. The six stages are completed right after project exploration, during project definition and design, during design and procurement, during construction and safety check, and during normal operation.

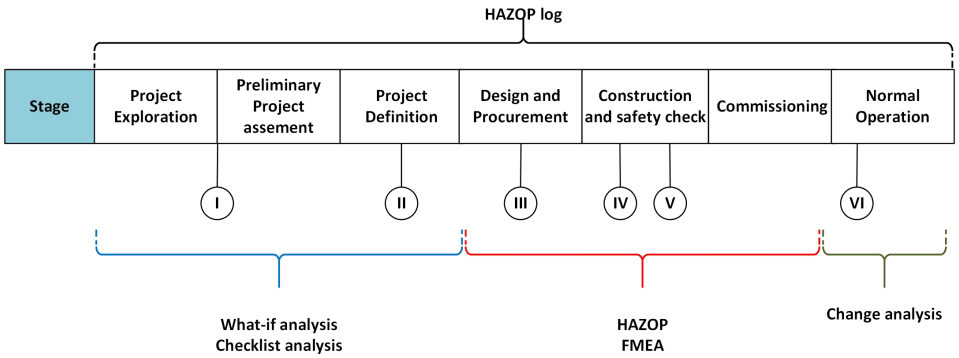

Figure. 3.4 *Six stages lifecycle for process hazard analysis [19] and divers hazard identification methods*

In different stage, there are several applicable methods for hazard identification. In accordance with the outcome of literature review of hazard identification methods, some methods can be particular beneficial for certain stages in project development, particularly for process industry. What-if, checklist analysis may be suitable for the hazard analysis (I and II) during stages of project exploration, preliminary project assessment and project definition. While hazard analysis (III, IV and V)

can use HAZOP and FMEA, change analysis may always be adopted during normal operation. For a HAZOP log, it is living document, which is updated during the entire life cycle of a system or plant.

As a summary, the primary finding is that few hazard identification methods can be individually utilised to look into the hazard event that is caused by simultaneously occurring safety trips. If there is a method to serve the purpose, the advantages and pitfalls of the method may be a topic of interest to risk analysts and SIS designers as well. Moreover, "when the analysis of dangerous combination of output states of SIS should be executed during process design" can also be discussed.

3.4 Allocation of Safety Functions to Protection Layers

Besides hazard and risk assessment, allocation of safety function is an essential phase to determine SIL and provide input to SRS. A number of methods about SIL determination for SIFs are suggested in IEC61511 [2], including risk matrices, risk graph, and layers of protection analysis (LOPA) (refer to Annexes B-F of Part 3 of IEC61511 [2]). The example here is given by LOPA, which has been evaluated as a practical method for SIL allocation. Based on the interfaces with HAZOP, it attempts to point out the problem, if the most commonly accepted hazard identification methods is not able to uncover the specified hazard. Consequently, the SIS design in process industry perhaps does not fully comply with the requirements in IEC61511 [2], Chapter 10.3.

3.4.1 Layer of Protection Analysis

Layer of protection analysis (LOPA) can be viewed as a special type of event tree analysis (ETA), which has the purpose of determining the frequency of an unwanted consequence that can be prevented by a set of protection layers. The approach evaluates a worst-case scenario, where all the protection layers must fail in order for the consequence to occur. The frequency of the unwanted consequence is calculated by multiplying the PFDs of the protection layers with the demand on the protection system (represented as a frequency). Comparing the resulting frequency of the unwanted consequence with a tolerable risk frequency, identifies the necessary risk reduction and an appropriate SIL can be selected [25]. Figure 3.5 delineates the typical protection layers for a chemical process.

LOPA is a semi-quantitative method using numerical categories to estimate the parameters needed to calculate the necessary risk reduction which corresponds to the acceptance criteria [25]. In a quantitative risk assessment (QRA) mathematical models and simulations are often used to estimate the extent or escalation of damage, e.g. toxic diffusion, explosion expansion or fire escalation. In addition, FTA

or other methods are used to calculate the frequency of the accidental event [13]. In LOPA, simplifications, expert judgement and tables are used to estimate the needed numbers [25]. LOPA usually receives output from a HAZOP or a hazard identification study (HAZID) and often serve as input to a more thorough analysis as a QRA. For the method of LOPA, the reference can be made to [25].

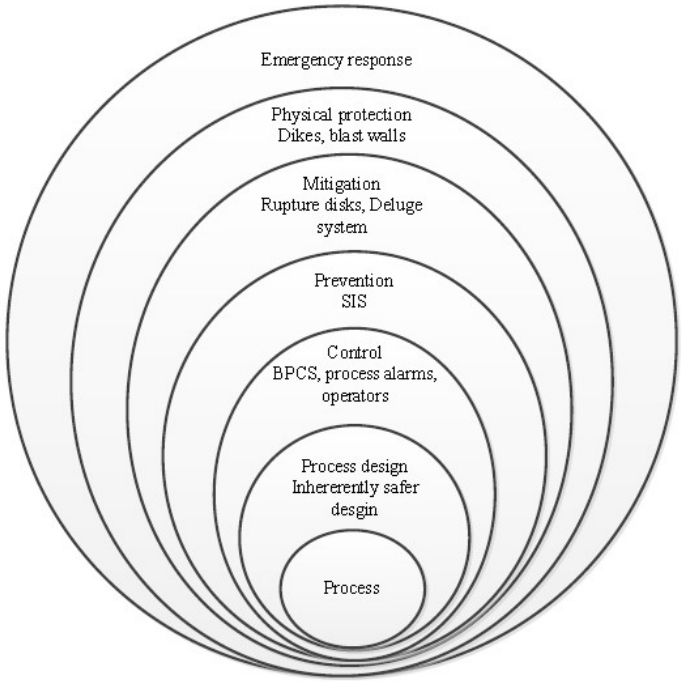

Figure. 3.5 *Protection layers [2]*

Figure 3.6 shows the interaction between the HAZOP and LOPA worksheets. The main concept is referred to a master thesis "Layer of Protection Analysis (LOPA) for Determination of Safety Integrity Level" [28]written by Christopher A. Lassen in 2008 for his master degree from NTNU. LOPA is performed from the left to the right in the worksheet and receives input from the HAZOP during the analysis. The consequence identified in the HAZOP answers to the impact event in LOPA, and possible cause from HAZOP are the initiating causes in LOPA. Meanwhile, the arrows are blue and dotted, which indicates that the information from the columns including safeguards and actions required cannot be transformed directly. The HAOZP consequence severity ranking (S), and the HAZOP consequence likelihood (L) can be transformed to LOPA, and impact event severity level and initiating cause frequency are the applicable terms in LOPA with associated columns. The HAZOP worksheet does not have to include the columns of severity racking and likelihood, but there are must be evaluated prior to a LOPA. Therefore, the blue

dotted lines in Figure 3.6 indicate that evaluation is need when transferring data to LOPA. The detailed information about relationship between HAZOP and LOPA worksheet is not discussed in this case. The key point is that both HAZOP and LOPA do not uncover the hazard due to simultaneously occurring safety trips. In order to involve this kind of information in SRS, it requires a specific hazard identification methodology, which has not been mentioned in any research in both academia and industry.

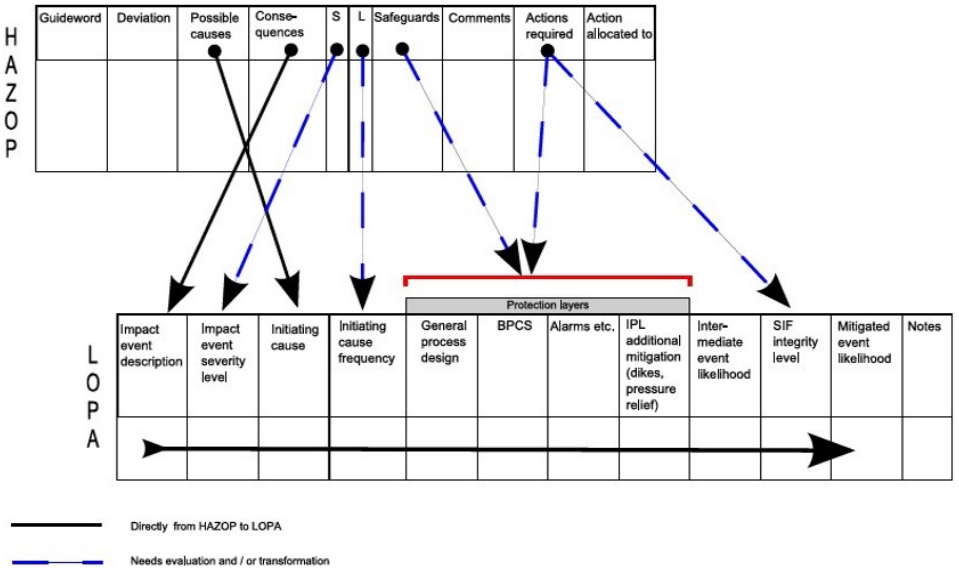

Figure. 3.6 *Relationship between HAZOP and LOPA worksheets [28]*

4 Methodology for Identification of "New Dangerous States"

Following the ideas mentioned in Chapter 1, a three-step recipe is proposed in order to identify dangerous combinations of safety trips in a technical system. It consists of:

Step 1: Carry out system breakdown.

Step 2: Identify dangerous combinations of safety trips.

Step 3: Perform dynamic simulations.

It should be noted that each step mentioned above is going to be treated individually. The detailed procedure will be introduced in the following. Prior to that, the definition of new dangerous states and essentials of identification of this type of state during process/plant design is presented.

4.1 New Dangerous States

The objective of a SIF is to bring EUC into a safe state or to keep EUC in a safe state when a demand occurs in order to protect people, environment, and material assets. A safe state is a state of EUC, whether the system is operating or shut down, such an undesired event cannot occur. Meanwhile, the safe state must be achieved in a timely manner. In process industry, the time allowed to bring the process to a safe state is called the *process safety time*[1] . It is the time available from detection until the SIF must be completed in order to avoid an escalation. In process industry, the safe state is often achieved by shutting down the process.

A new dangerous state here means the dangerous state due to combinations of output states of the SIS. This type of dangerous state may be difficult to be detected

[1]Process safety time is the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed. [2]

or understood since a SIF is considered in terms of process/plant safety. In addition, it is also impossibly identified in the manufacturing phase of SIS, since it merely becomes obvious when the SIS is implemented in a process or plant. However, the information package of SIS product provided by SIS vendor is inevitable to support the identification of this type of dangerous state. It seems necessary for all personnel in the plant/process design team as well as SIS vendors to be aware of the existence of this type of new dangerous state or may be also called "hidden unsafe state". In the following, it is the description of methodology, which intends to identify the new dangerous states in technical system, particularly chemical process industry.

4.2 Step 1: Carry Out System Breakdown

The intention of this step is to break down the overall system into subsystems that can be handled effectively and be analysed individually.

A system breakdown should focus on the overall *information flow diagrams*. In this case, the information flow diagram can be interpreted as the overall architecture of engineering design, such as data flows in computer science and networking, electrical currents shown in circuit diagrams in electronics, and fluid flow and processing as depicted in process flow diagrams in a typical chemical plant. One example of information flow diagram is illustrated in Figure 4.1.

Process flowsheets are the language of chemical processes. They describe an existing process or a hypothetical process in sufficient detail to convey the essential features. A process flowsheet is a collection of icons to represent process and arcs to represent the flow of material to and from the units. It emphasizes the flow of material and energy in a chemical process.

It is possible to automate partitioning of network by using algorithms that typically present in modular process flowsheet simulator[2]. Gundersen and Hertzberg gave a review of such algorithms in [29]. Partitioning is to locate with a flowsheet the group of units, which must be solved together (called irreducible groups) with as fewest number of units as possible [29]. Among different algorithms for breaking down a flowsheet, path tracing algorithm by Sargent and Westerberg (1964) [30] has been widely applied due to the simplicity. In essence, the Sargent-Westergerg algorithm traverses a graph to identify all loops. One traces from one unit to the next through the unit output streams, forming a 'string' of units. This tracing continues until

[2]In order to interpret process flowsheets, locate malfunctions, and to predict the performance of process, process simulation plays essential role in process design and optimization. To perform process simulation, a process simulator is utilized, which converts a process flowsheet to a simulation flowsheet, i.e. replace the process units with appropriate simulation unit. Meanwhile, a process simulator enables to model and solve the process unit equations, while a subroutine is written for each process unit.

1. A unit in the string reappears. All units between the repeated unit, together with the repeated unit, become a group, which is collapsed together and treated as a single unit, and the tracing continues from it.

2. A unit or group of units without no more outputs is encountered. The unit or group of units is placed at the top of a list of groups and is deleted entirely from the problem.

The steps of path tracing algorithm is not explained in details, because it is mentioned here to solely provide a fundamental knowledge of partitioning flowsheet. The main intention is to propose a new algorithm for system breakdown in the methodology of identification of new dangerous states.

It is fact that parts of the information flow graph containing loops will have strongly interacting input-output mappings, which makes it necessary to solve the mass and energy balances for these units simultaneously. Based upon this, a critical assumption is made on time-scales of dynamic responses.

Assumption:

The new hazard event resulting from simultaneous trips is only considered, when a same time-scale is utilized for determining the leading effects on process or plant.

This assumption illustrates that slowly developing changes in the plant, e.g. due to large recycle flows are assumed to be handled by individual safety trips and not to be seen as an effect of multiple trips occurring at the same time. The reason is that effects propagating through the plant will affect every unit in the loop one by one, and will be limited by the hold-ups of the plant. Figure 2.4, in Chapter 2 can be used as a simple illustration, which depicts a distillation column connected to a continuous stirred-tank reactor (CSTR). Holding the reactor level constant may cause variability to go through the entire plant and may cause the whole plant to oscillate. Such effects are supposed to be discovered at individual unit level by applicable localized analysis, such as a HAZOP study.

Based on the concept of path tracing algorithm and the assumption with respect to the same time-scale, a suggested heuristic for analysing flowsheet is given as follows:

1. Define the scope of analysis, and collect the process flowsheets of addressed subject.

2. Identify all loops within the process flowsheets.

3. Develop the list of subsystems that will be analysed. There are three rules in order to prepare the list of subsystems.

- ***Rule a)*** If nested loops exist, the time-scales of the plant should be considered. For a few units that interact strongly on a short time-scale, label those units into a group to be analysed and recorded as one subsystem. Disregard large loops with relatively massive holdups due to time-scale separation. It

should be claimed that there is no standard definition of the time scale, which needs to be determined by engineer's experience.

- ***Rule b)*** Any two neighbouring units should be analysed together.

- ***Rule c)*** Consolidate subsystem list by removing subsystems that are overlapped in other subsystems in the list.

This procedure will break down the problem into a manageable size of sub-problems to a certain extent. However, this does not give any guarantees to completeness. The analyst may adopt spot checks[3] to check if other systems should be included in the screening design as well, but this activity will not be discussed further in this project.

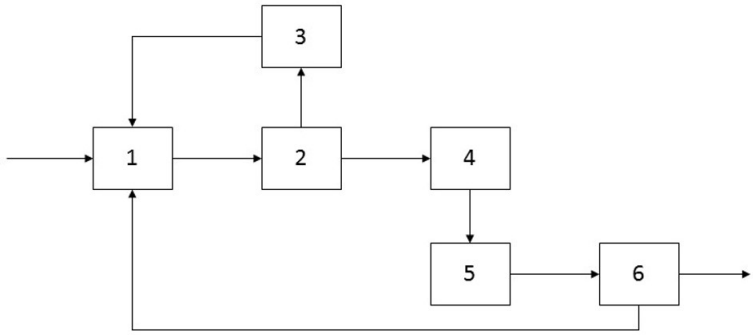

Figure. 4.1 *An example of information flow diagram*

The illustration in Figure 4.1 is taken as an example to demonstrate the procedure of system breakdown, while the information flow diagram is partitioned in accordant with the rules mentioned above. First of all, all the loops on the process flowsheet are confirmed. At first glance, there are two nested loops, which are {1,2,3} and {1,2,3,4,5,6}. The latter is considered as a large loop, which will be disregarded immediately due to Rule a). {1,2,3} is labelled as a group and temporarily recorded as one subsystem on the list. Furthermore, {1,2,3,4}, {4,5} and {5,6} are discovered according to Rule b) and recorded on the list of subsystems as well. Since the subsystem {1,2,3} is contained within subsystem {1,2,3,4}, the redundant subsystem {1,2,3} is eventually disregarded with respect to Rule c). Therefore, only subsystem {1,2,3,4} {4,5} and {5,6} will be analysed in next step of analysis. The list of subsystems is described in Table 4.1.

[3] A test made without warning on a randomly selected subject.

Table. 4.1 *List of subsystem based on the step of system breakdown*

Subsystem	Comments
{1,2,3}	According to Rule a) and delete because of Rule c)
{1,2,3,4}	According to Rule b)
{4,5}	According to Rule b)
{5,6}	According to Rule b)

4.3 Step 2: Identify Dangerous Combinations of Safety Trips

For each subsystem defined in Step 1, select safety trip pairs and apply guidewords to identify if simultaneous activation will yield a response that pushes the plant towards its design limits.

The main purpose of the second step is to identify whether output combinations of safety trips may be dangerous within each subsystem. This can be achieved by applying guidewords, while the analysis can be similar with a HAZOP study.

The basis of analysis includes:

1. Within one subsystem, all possible pairs of trips that may occur simultaneously should be listed. Reference can be made to standards or industrial guidance, i.e. ISO 10418 (2003) [11] and API RP 14C (2007) [31], while the quality of the list depends on the engineers' experience.
2. All trips that have the same effect on the process should be deleted from the list. In other words, safety trips have the same final elements should be excluded from the list. In order to achieve it, the cause and effect (C&E) diagrams[4] or SRS tables may be used as references.
3. For the remaining pairs of trips, apply the parameters and guidewords from Table 4.2, which is exactly the same as the parameters and guidewords applying in a HAZOP study [7]. If a physical response of the plant may push the plant in the direction of design limitations, the pair of trips should be marked as "scenario for dynamic simulation". In addition, the probability of event (the assessment of probability is introduced in Chapter 5) is also necessary to

[4]The C&E diagram is not the well-known "fishbone diagram" [6] that is usually used as a method of casual and frequency analysis in brainstorming session. In comparison, the C&E diagram here is a type of design documentation, which is particularly developed for process design inspection. The frame of the documentation is similar as depicted in Table 4.3. For different companies, there may be various preferences for documentation, but the main idea is more or less the same.

be taken into account. If the probability is considered to be sufficiently low, the event may be neglected. Once it is confirmed as non-negligible event, the pair of trips should be documented in the worksheet together with explicit explanation of the reason why the trips is included in the worksheet, i.e. possible consequence of trip activation. An example of the worksheet is depicted in Appendix A.

4. Repeat 1), 2) and 3) for all remaining subsystems. A summary of all such events should be made for inclusion in the safety requirements specification (refer to Chapter 1).

Table. 4.2 *Parameter and guidewords for a HAZOP study*

Parameter	**Guideword**
Pressure	High
	Low
Flow	High
	Low
	No
	Reverse
Temperature	High
	Low
Level	High
	Low
Loss of containment	

As an illustration, a sketch of a CSTR connected with a distillation column is drew in Figure 4.2. It assumes each process unit is installed with level alarm high high (LAHH) and level alarm low low (LALL). There three process shutdown (PSD) valves, XV1, XV2 and XV3. XV 1 is final element of LAHH in Unit1, and XV2 automatically closes if LALL in Unit1 is triggered. Analogously, XV 2 is also final element of LAHH in Unit2, and LALL in Unit2 trips XV3 when it is on demand. While XV1 and XV2 are located in the feed inlet and outlet of Unit1, respectively, XV2 is installed in outlet of Unit2. There is a recycle loop coming from distillation column to reactor in order to return unreacted reactants.

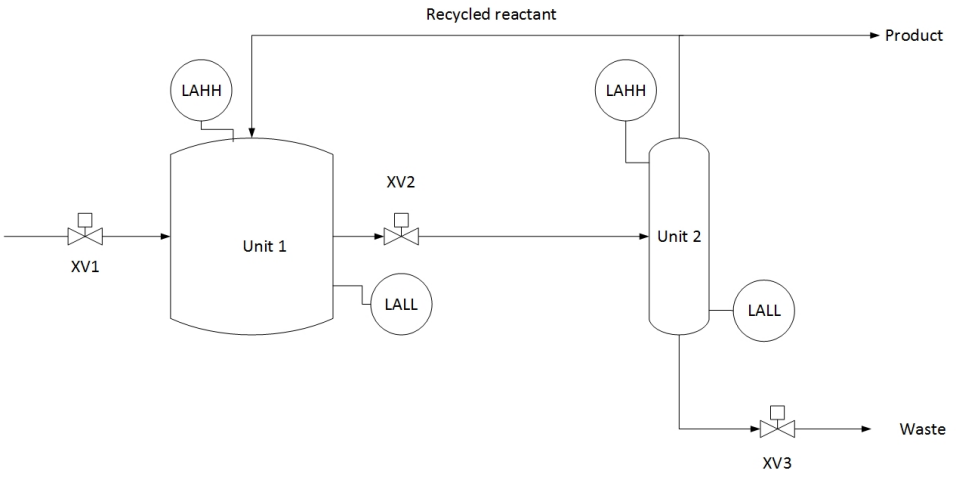

Figure. 4.2 *A CSTR connected with distillation column*

Based on the description, all possible combinations of safety trips can be listed as follows:

- {LAHH in Unit1,LALL in Unit1 };
- {LAHH in Unit1,LAHH in Unit2 };
- {LAHH in Unit1,LALL in Unit2 } ;
- {LALL in Unit1,LAHH in Unit2 };
- {LALL in Unit1,LALL in Unit2 } ;
- {LAHH in Unit2,LALL in Unit2 } ;
- {LAHH in Unit1,LALL in Unit1,LAHH in Unit2 } ;
- {LAHH in Unit1,LALL in Unit1,LALL in Unit2 } ;
- {LALL in Unit1,LAHH in Unit2,LALL in Unit2 } ;
- {LAHH in Unit1,LALL in Unit1,LAHH in Unit2,LALL in Unit2 }

The task is to remove the trips that have the same effect on the process or, in other words, have the same final elements. Final element of each safety trip can be seen in Table 4.3. Table 4.3 can be regarded as a simplified version of a formal C&E diagram. For simplicity, safety trips can be numbered according to the first column in Table 4.3. Combination of trip 2 & 3 can be disregarded, since they share the same final element, XV2. Consequently, combinations of trips should be taken into further consideration including {1,2}, {1,3}, {1,4}, {2,4}, {3,4}, {1,2,4} and {1,3,4}.

The next step is to apply guidewords, such as "pressure high" "pressure low" (see in Table 4.2) on each combination of safety trips. The analysis can not be demonstrated here due to lack of detailed information of process, such as types of process units, the characteristics of reaction.

Table. 4.3 *C&E diagram*

No.	Trips	XV1	XV2	XV3
1	LAHH in reactor	X		
2	LALL in reactor		X	
3	LAHH in distillation column		X	
4	LALL in distillation column			X

Moreover, the expected result of Step 2 should be a list of combinations of safety trips that are considered for dynamic simulation. The "HAZOP exercise" should be documented as a standard HAZOP worksheet, and a list of scenarios that is considered in dynamic simulations should be distilled from those results. One difference from typical HAZOP is that the "cause" is replaced by the pair of trips occurring at the same time. The following task becomes to find out if it could cause a high/low pressure, high/low temperature and so on. An example of worksheet format is recommended in Appendix A. If probability assessment is needed or it is not obvious whether the effect is significant or not, the analysis should be carried out separately and returned to the worksheet to complete documentation.

The analysis has so far come up with a list of combinations of safety trips, for which a new risk containment measure is indispensably introduced. Dynamic simulation is treated as essential method to draw the conclusion. The next step is to set up the description of simulation cases for each identified pair of safety trips.

4.4 Step 3: Perform Dynamic Simulations

The main intention of this step is to:

1. Perform dynamic simulations for scenarios that are identified in Step 2.
2. Find out the candidates, which may actually result in a new dangerous state.

The dynamic simulation must be able to answer the question:

From any starting point where safety trips are occurring at the same time, does the combination violate the design limits of the process or plant?

Dynamic simulation is an extension of steady-state process simulation[5] whereby time-dependence is built into the models via derivative terms i.e. accumulation of mass and energy. In other words, dynamic simulation uses mathematical models that describe how various properties of a given system are changing in time [33]. The unsteady-state conservation of a certain property can be expressed by the following general equation [32]:

$$\begin{Bmatrix} Accumulation \\ rate \end{Bmatrix} = \begin{Bmatrix} Input \\ flows \end{Bmatrix} - \begin{Bmatrix} Output \\ flows \end{Bmatrix} + \begin{Bmatrix} Generation \\ rate \end{Bmatrix} - \begin{Bmatrix} Consumption \\ rate \end{Bmatrix} \tag{4.1}$$

In general, the models used for dynamic flowsheeting consist of mass, energy and momentum conservation equations. When chemical reactions take place, it is useful to work with number of moles instead of mass. Because the momentum (Navier-Stokes) equations are difficult to solve, they are usually replaced by a flow hypothesis, for example perfect mixing or plug flow [33].

Moreover, the advent of dynamic simulation indicates the time-dependent description, prediction and control of real processes in real time has become possible, which includes the description of starting up and shutting down a plant, changes of conditions during a reaction, holdups, thermal changes and more [34].

There are various solution tools available for dynamic simulations. The set of differential and algebraic equations can be solved numerically. Simple models can be solved by implementing the Euler method in Microsoft Excel[6] . General-purpose mathematical software as Mathworks Matlab[7], Maplesoft Maple[8], Wolfram Research Mathematic[9] asks the user write the mathematical model and to call an ordinary differential equations (ODE) or differential-algebraic equations (DAE) solver. For more difficult problems, one can use high level programming language such as FORTRAN or C++ together with appropriate numerical libraries, such as Rogue Wave IMSL[10], Numerical Algorithm Group (NAG)[11] or available from free sources such as Netlib repository[12]. More specialized dynamic process modelling software package are PSE gPROMS[13], AspenTech Aspen Dynamics, Aspen Custom Modeller and HYSYS[14]. These package comprehensive facilities for developing, validating and executing dynamic models of chemical processes. Activities such as steady-state and dynamic simulation, operation and parameter estimation can be

[5] Process simulation was initially used to simulate steady state processes. Steady-state models perform a mass and energy balance of a stationary process, which is a process in an equilibrium state [32]. It does not depend on time.

[6] Office.microsoft.com

[7] www.mathworks.com

[8] www.maplesoft.com

[9] www.wolfram.com

[10] www.roguewave.com

[11] www.nag.co.uk

[12] www.netlib.org

[13] www.psenterprise.com

[14] www.aspentech.com

performed. Libraries of model for the most common unit operations are included, as well as support for calculating physical properties. Normally, dynamic simulation is executed with specialized dynamic process modelling software in reality. HYSYS is the mostly common solution tool adopting in Oil & Gas industry, while line-based chemical industry shows strong preference of applying Aspen Dynamics.

However, it is a fact that dynamic simulations, which are mathematically more complex than a steady state simulation, require increased calculation time. Since the late 1990s dynamic simulation has become a generally accepted tools by process engineers and control engineers [10]. Thanks to the software available today, it enables process engineers with process control knowledge and control engineers with process knowledge to build dynamic models easily [33]. The limitation in using dynamic simulation is no longer the difficulty in configuration. Nevertheless, the implementation time for a dynamic model is still two to four times as long as the time needed to implement a steady model [10]. It is normal that a consultant is engaged to develop the model and one or more engineers of an operating company use the model to perform relevant studies.

In the methodology of identification of new dangerous states, dynamic simulations do not necessarily need to utilize a full plant model. As the information flow graph is already simplified in the first step of analysis, the identified subsystems can be used as boundaries for dynamic simulations. It is supposed to significantly reduce the complexity of simulation, while the idea is the same as partitioning a flowsheet to reduce computational effort of complex flowsheets with many recycles during process simulation.

Based upon the description of three-step method, a worksheet of identification of new dangerous state is illustrated in Figure 4.3.

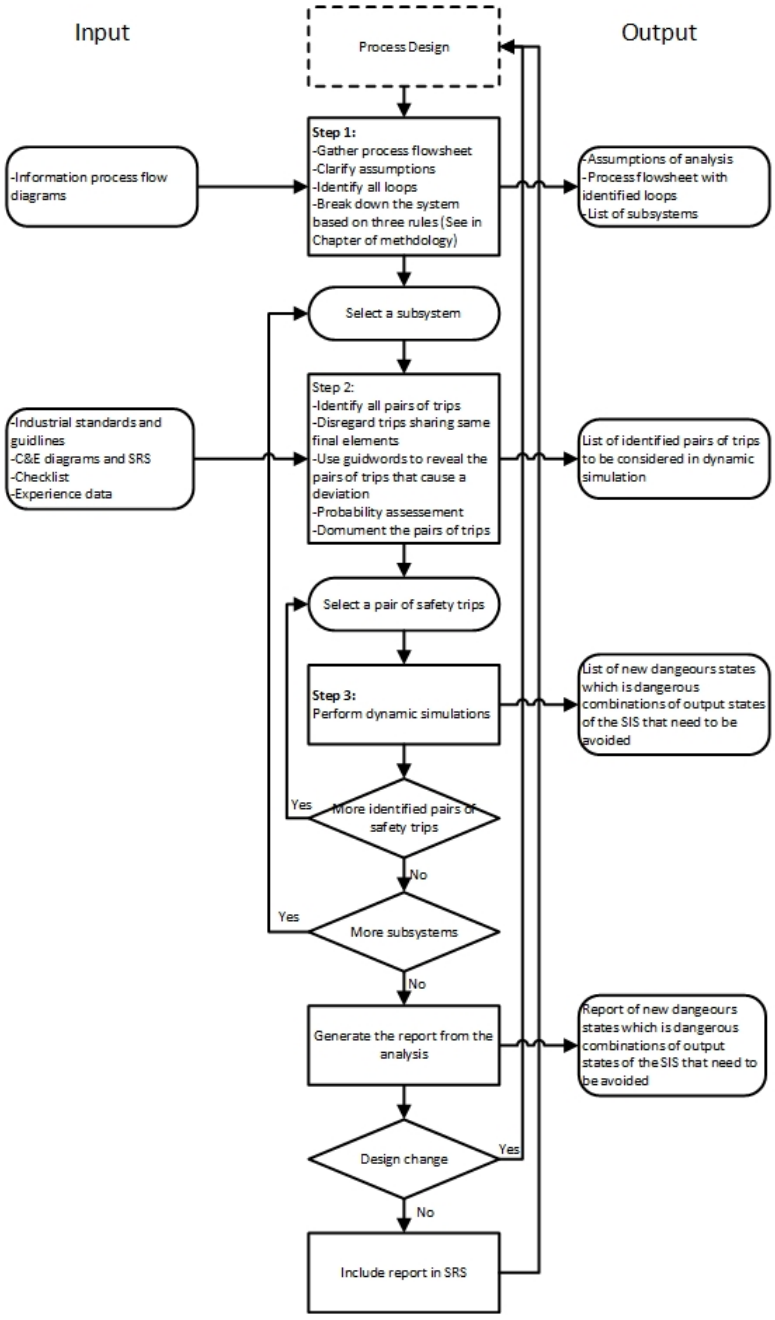

Figure. 4.3 *Worksheet of analysis*

5 Suggested Work Procedure for Probability Assessment

5.1 Introduction to Probability Assessment

The probability of the occurrence of simultaneous safety trips could be so low that the risk would be mostly deemed "acceptable[1]", if the events are considered statistically independent. However, most of the events are not statistically independent because of the dependent failures[2] such as common cause failure, cascading failure and negative dependencies [13].

Framework for assessing the probability of dependent events is indispensable in the proposed methodology (see Chapter 4). There are a number of theoretical approaches available for the probability assessment of system reliability [13], which are not independent from a statistical point of view. While most available ones are rigorous and relatively complex, a simple and efficient method is demanded since the task of probability assessment is part of a "screening tool". In addition, it is necessary to emphasize the differentiations between two levels of probability, significant and insignificant.

It is popular among risk analysts to use a semi-quantitative method for establishment of risk reduction requirements [2], including safety integrity levels. Such methods typically have the right granularity with assumption of statistical independence of events: a chain of events is analysed by multiplying probabilities of each barrier function failing. The logic does not apply to dependent events. In order to demonstrate the method of probability assessment of simultaneous trips within a subsystem, a simple illustration, along with the suggestions of probability assessment as parts of screening tool, is described in the following.

[1] Acceptable risk means the risk is accepted in a given context based on the current values of society and in the enterprise. [6]

[2] This master thesis only focuses on common cause failure rather than others.

5.2 Probability Assessment of Simultaneous Safety Trips

A CSTR producing a liquid product is considered as an example. The reactor is designed with a cooling jacket using refrigerant, since the reaction is exothermic. Cooling stream is injected by a cooling medium pump. A basic process control system is installed in CSTR to keep the temperature within a pre-set limit. In addition to basic process control system, a level alarm low low (LALL) is installed to hold liquid level in CSTR if the liquid level exceeds minimum allowable level. If LALL is initiated, a process shutdown valve located in product outlet is automatically closed. Moreover, the cooling system has a PALL alarm. If a too low pressure is detected in cooling system, a process shutdown valve in inlet of cooling system will terminate cooling stream. The layout of the system is visualized in Figure 5.1.

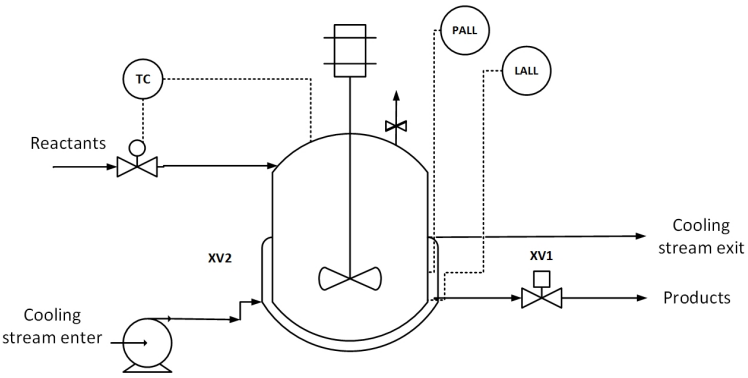

Figure. 5.1 *The layout of process consisting of a CSTR and cooling system*

The case is that a cooling system trip is triggered to stop the flow of refrigerant at the same time as a low level trip occurs within the CSTR. The situation would lead to increased residence time (outflow stops) and a loss of cooling occurs. This will potentially result in over temperature and over pressure in the CSTR. As a reaction, the safety functions of both level alarm low low (LALL) in reactor and pressure alarm low low (PALL) in cooling system will be on demand. A simplified analysis of the demands on these safety functions is presented including causes analysis and probability assessment.

Causes Analysis

In order to analyse the causes of two events "reactor level alarm low low (LALL)" and "cooling system pressure alarm low low (PALL)" (for detailed information see standard [35]), the fault tree analysis is applied. The result of the analysis is depicted in Figure 5.2.

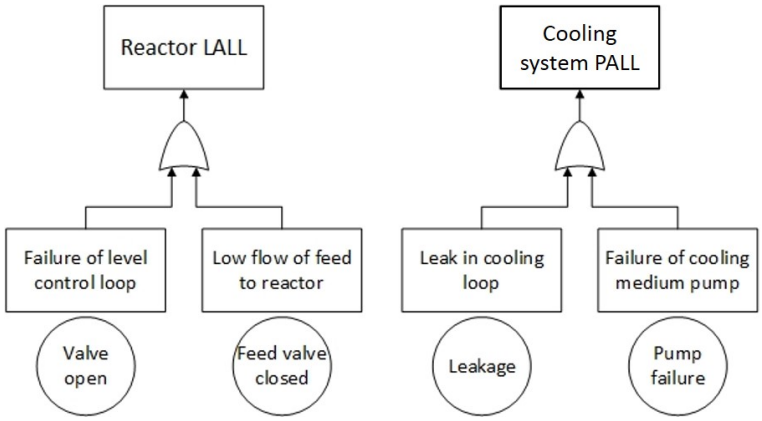

Figure. 5.2 *Results of cause analysis*

It shows that two top events do not share any common causes.

Probability Assessment

The reactor LALL demand rate is:

$$\lambda_{LALL} = \sum_i \frac{1}{MTTF_i} = 0.1 + 0.1 = 0.2 \tag{5.1}$$

The cooling system PALL demand rate is:

$$\lambda_{PALL} = \sum_i \frac{1}{MTTF_i} = 0.01 + 0.1 = 0.11 \tag{5.2}$$

If assuming all of these events are statistically independent, the expected demand rate on the functions combined would be $\lambda \approx 0.1 \times 0.2 = 0.02$ This means that the probability of a combined demand is 2% for any given year.

Common Causes

Consider now a situation where common causes exist for both trips to be set off. Then these must be kept out of the multiplication done above, and added separately. This would increase the demand significantly.

5.3 Suggested Work Procedure for Probability Assessment

A probabilistic assessment should be done in as simple as possible with enough rigor to assess whether further work is needed. To evaluate whether the probability of a pair of trips being activated simultaneously is sufficiently high to warrant further investigation with dynamic simulation, the following approach is suggested:

1. List all demand causes for each trip.
2. Separate them into ”independent” and ”common causes”.
3. Summarize independent causes for each trip and multiply those demand rates, add common causes demand rate to get an overall estimate on the demand rate for the pair of trips.
4. If the demand rate significantly influences the risk level of the operation, perform dynamic simulations and propose design mitigation actions.

A possible definition of ”significant” is within 10% of the PFD (probability of failure demand) of the highest SIL requirement for the two trips considered. A worksheet of probability assessment of simultaneous safety trips is suggested in Figure 5.3.

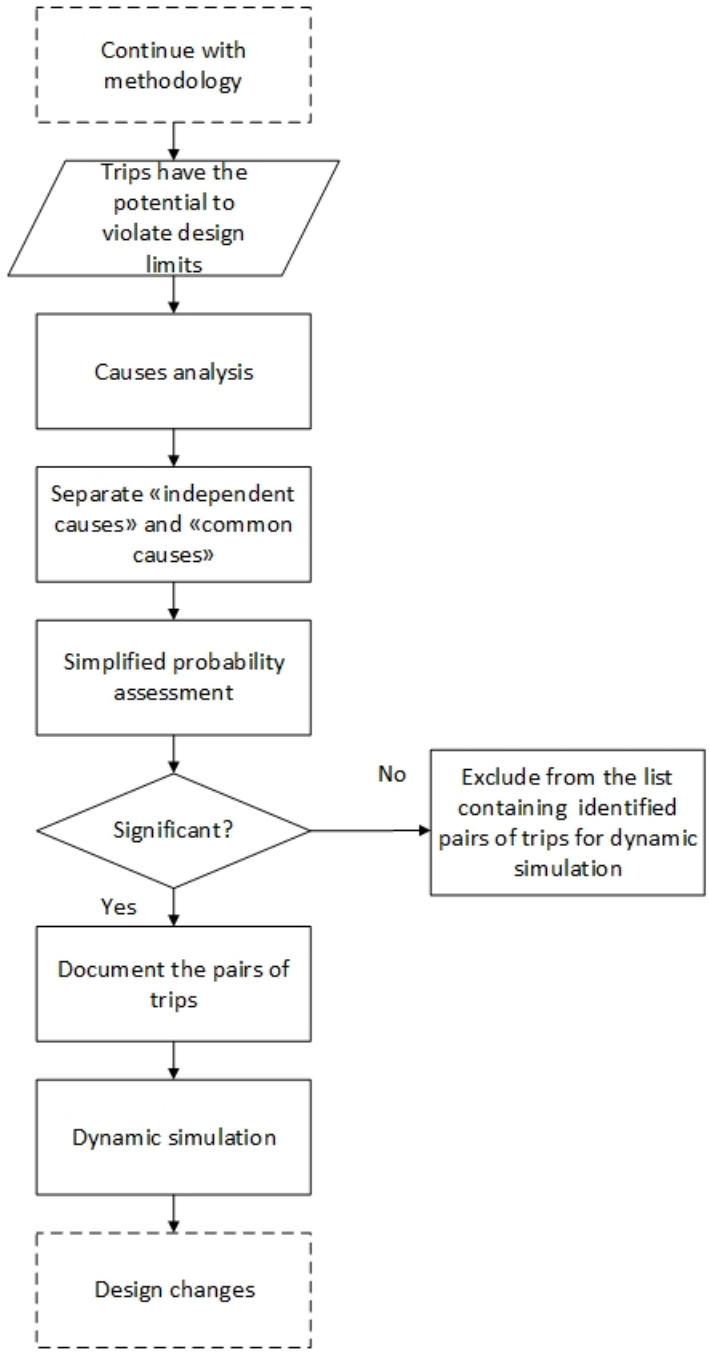

Figure. 5.3 *A suggested work procedure for probability assessment of simultaneous safety trips*

6 Case Study 1: Flow Network With Multiple Releases to Flare Header

6.1 Introduction to Case Study 1

The methodology established in this master project is a generic methodology that can be applied to identify, if a system has the potential to generate a hazard since several individual safe states occur simultaneously in the process. Dynamic simulation plays a critical role in the method. In this chapter, a case study is presented with the use of a commercial dynamic simulator, *OLGA* Flow Assurance. The purpose is to capture the transient process with comparison between full blowdown and BDVs opening with a time sequence. It also attempts to reveal that the specified problems typically occur in interconnected flow networks (typically processes with mass and energy integration).

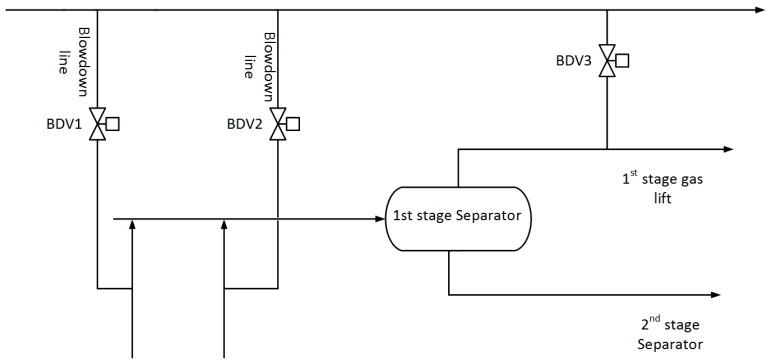

Figure. 6.1 *An example of flow network with multiple releases to flare header after tie-in of new producers*

Driven by economic benefits, more and more subsea-wells are tied in offshore platforms nowadays. Making sure a proper time sequence of BDV initiations is inevitable for the design and modification of blowdown and flare system. In order to estimate the effect of different blowdown scenarios in flare header on topside platform, the simulation is based upon a system, which consists of a multi-well production facility with multiple blowdown lines. Riser, inlet arrangement and the separation system of a typical oil production facility will be used as the case study. Figure 6.1 demonstrates an example of flow network with multiple releases to flare header after tie-in of new producers.

6.2 Dynamic Simulation for Flare System Design

Gas flaring is a common practice in the Oil & Gas industry during process upsets [36]. As a critical safety requirement at oil and gas installations such as refineries and process facilities, a flare system is usually installed to relieve built up that may occur during shut down, start up or due to process system failure, reducing other safety hazards associated with process emergencies [21] [35] [37].

Thermo-hydraulic modelling serves a key role in flare system design. It enables the estimation of the thermodynamic and hydraulic parameters such as pressure, temperature, velocity/Mach, and other flow parameters required for building/modification of flare system. It is a tendency to involve dynamic simulation in the design of flare system by using commercial dynamic simulators such as Aspen HYSYS[1], K-spice[2] and *OLGA*[3]. Compared with conventional steady-state tools particularly tailored for flare header design, i.e., Aspen Flare System Analyser[4], Flaresim[5] and g-Flare[6], dynamic simulators have been considered as useful in characterizing the transient process accompanying different process relief scenarios, i.e. during blow-down. In addition, dynamic simulators enable to generate a clear representation of how the flow-rate, pressure, temperature would change with time. There have been some achievements in relevant research work [38] and some are under progress in academia with cooperation from industry [39]. The detailed variation versus time during the process offer a better perspective to the designer, which will definitely contribute to the improvement of flare system design.

[1] http://www.aspentech.com/hysys/
[2] http://www.kongsberg.com/en/kogt/products%20and%20services/production%20assurance/
[3] http://www.software.slb.com/products/foundation/Pages/olga.aspx
[4] https://www.aspentech.com/products/engineering/aspen-flare-system-analyzer/
[5] http://www.softbits.co.uk/fsoverview.php
[6] http://www.psenterprise.com/oilandgas/gflare.html

6.3 Flare System

The flare system (Figure 6.2) is the single largest pipe network on an offshore production platform. It serves as a relief system for depressurizing different process and production units in cases of shutdown or unexpected cases of hazardous process emergencies, by collecting excess fluid through relief devices and a pipe network and disposing of it to the required outlet.

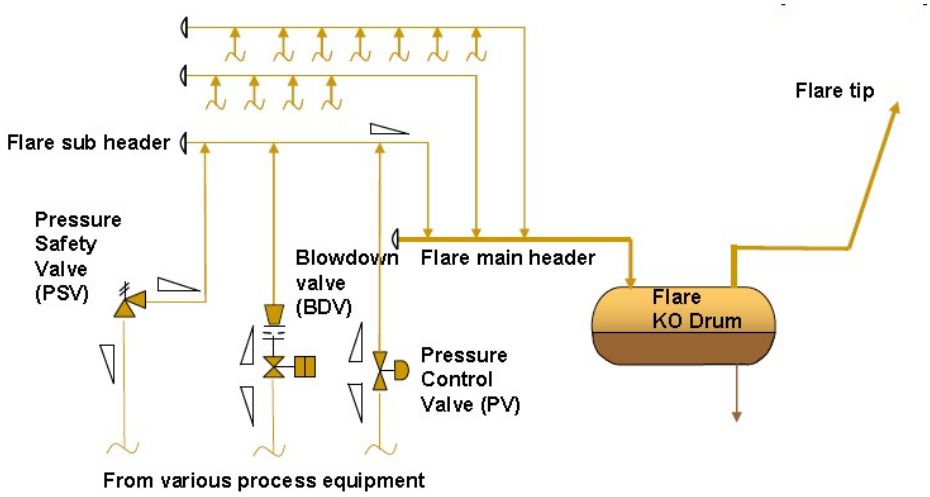

Figure. 6.2 *An illustration of a typical flare system [39]*

A flare system consists of different relief units that handle depressurization for the different processes taking place on the platform, to ensure safety of life and property on it. Typical sources of process relief are the production manifolds, compression system and separations where it is possible for pressure to build up/overpressure. The relief systems includes process relief, process flaring, blow-down etc [38].

Process Relief

Process relief involves pressure relief of a process unit in case of overpressure due to a process upset. Overpressure may occur due to heat input, which increases pressure through vaporisation and/or thermal expansion; and direct pressure input from higher pressure sources. In order to ensure process safety, pressure relief devices are connected to the vessels and units with a potential for overpressure.

Process Flaring

Process flaring involves the controlled flaring or bleeding out of gas from a particular process unit or compressor, in case of pressure build up above the acceptable limits. This is in order to allow for continued production, without causing a process upset from build up of pressure. Pressure control valves (PCV or PV) are used for process flaring.

Blow Down

Blow down is the actual process of de-pressurizing a given process unit (separator/piping) after shutdown. A blow down valve (BDV) is used. In case of fire out break or related contingencies, the blow down valve opens up (is opened up) to release highly flammable fluids such as hydrocarbons from the separator or piping into the flare network. This serves as a safety measure against escalation of the fire into a full blow explosion.

6.4 *OLGA* Dynamic Multiphase Flow Simulator

OLGA Dynamic Multiphase Flow Simulator from SPT group is a well known and widely used flow simulation tool with many options of application from well flow to riser and pipeline flow simulation. *OLGA* can be run in both steady state and dynamic mode, making it an efficient and effective tool for simulating the many time dependent processes faced in the industry. In this master project, the simulation is based on *OLGA* (version 7.2.2).

6.5 Model

The model includes production riser, topside piping and valves, separators (both 1^{st} stage and 2^{nd} stage separator) including PSVs and flare system as shown in Figure 6.3.

Main inputs for establishing a model include:

- Fluid composition (i.e., gas, condensate, oil)
- Network topography (i.e., geometry)
- Pipeline data (i.e., diameter, materials of construction, insulation, heat transfer)
- Process equipment (i.e., separator, heat exchanger, valves)
- Boundary conditions (i.e., pressure, temperature, flow rate)

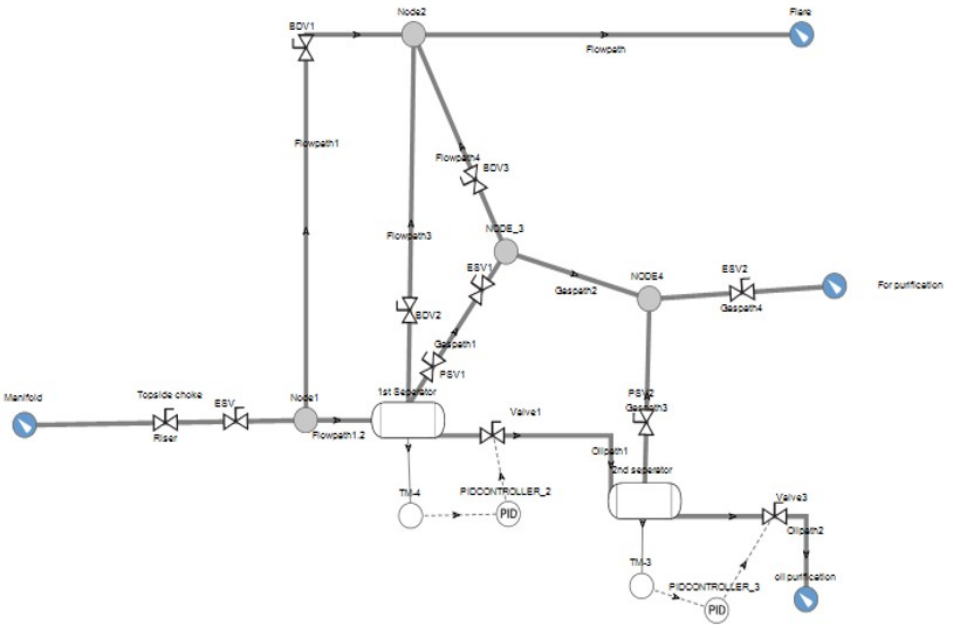

Figure. 6.3 *Screen shot of OLGA model for production riser and 1^{st} and 2^{nd} stage separator (The layout between subsea wells and manifold is omitted in model)*

6.6 Results of Simulations

6.6.1 Full Blowdown

Full blowdown means all BDVs open simultaneously in an emergency. Figure 6.4 delineates the trend plot of mass flow rate in flare line. During normal operation, which is before the first 1200 seconds in the case, BDVs are closed, and there is no flow in flare header. When three BDVs are triggered together at 1200 s, the value of mass flow rate suddenly rises up in flare line. At 1208 s, it reaches to about 1497 m^3/d. Following a short pause, it continues to increase at 1230 s, and retain around 1800 m^3/d during the period from 1300 s to the end of simulation.

During full blowdown, the trend of pressure in flare line is similar with mass flow in flare line. The result is plotted in Figure 6.5. During the first 1200 s there is almost no pressure in flare line. Since BDVs open at once, the pressure in flare line experiences a dramatic increase from 1 *bara* to the peak value of 8.87 *bara* within 10 seconds. Afterwards, it returns back a little and stays around 8.30 *bara* during the rest of simulation time.

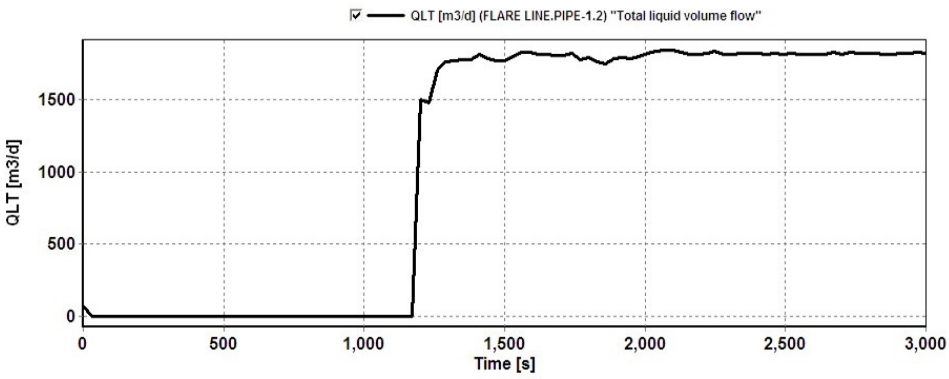

Figure. 6.4 *Mass flow rate in flareline during full blowdown*

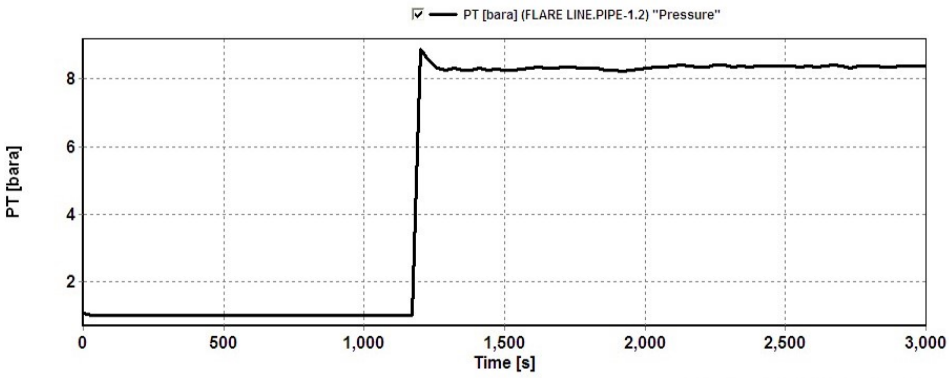

Figure. 6.5 *Pressure in flare line during full blowdown*

Note: *OLGA* calculates itself the pressure in a flow line due to boundary conditions although there is no flow until 1200 second. This explains why the value of pressure during normal operation was not zero.

Besides the mass flow rate and pressure in flare line, the transient process of pressures in 1^{st} stage and 2^{nd} stage separators are also observed with a safety concern. The result is illustrated in Figure 6.6. While the black and dashed line denotes the pressure in 1^{st} stage separator, the red and solid line represents the value of pressure in 2^{nd} stage separator. Due to full blowdown at 1200 s, the pressures in both 1^{st} stage and 2^{nd} stage separators dramatically drop down to a safe value before 1300 s. Finally, the values of pressure in 1^{st} stage and 2^{nd} stage separators are about 12.84 *bara* and 11.94 *bara*, respectively.

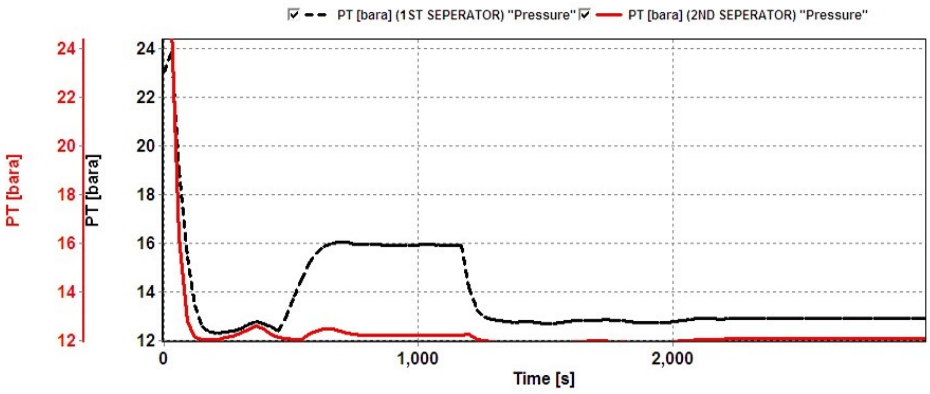

Figure. 6.6 *Pressure in 1^{st} stage and 2^{nd} stage separator during full blowdown*

6.6.2 Open BDVs with a Time Sequence

Differentiated with full blowdown, BDVs open in a series in this case. The interval between opening each BDV is set up with same value, which is 10 *min*. It means BDV1 is initiated at 1200 *s*. After 10 *min*, BDV2 fully open, and the last BDV opens at 2400 *s*.

The transient process of mass flow rate is demonstrated in Figure 6.7. Same as full blowdown, the mass flow rate increases quickly between 1200 *s* and 1230 *s*. Within 30 seconds, it gets to 1470 m^3/d, which is lower than the mass flow rate at 1230 *s* (1488 m^3/d) in the full blowdown case. Afterwards, the mass flow rate is stepped up. At each time when a BDV opens, there is a sharp increase in the mass flow rate in flare line. Following a temporary decline, it converges to a stable value, which is about 1800 m^3/d. The peak value, which is approximately 1872 m^3/d, appears at 2405 *s*.

Figure 6.8 depicts the pressure in flare line during blown valves opening within a time sequence. After a sharp increase, the pressure reaches to approximately 6.28 *bara* at 1236 *s*. Compared with full blowdown, 8.87 *bara* at 1210 *s*, 6.28 *bara* is obviously much lower. At 1800 *s* when the second BDV opens, the pressure experiences a sharp increase again, and a peak value, which is 8.57 *bara*, appears at 1801 *s*. Compared with full blowdown, the peak valve of pressure in flare line is dramatically decreased.

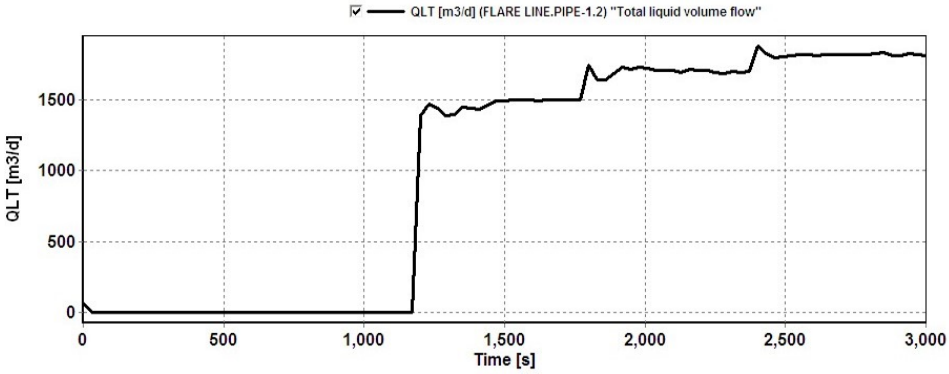

Figure. 6.7 *Mass flow rate in flare line during blowdown with a time sequence (10 min)*

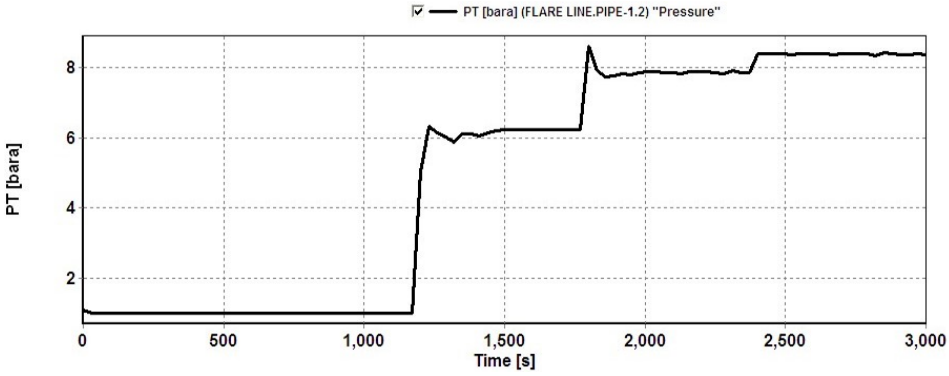

Figure. 6.8 *Pressure in flare line during blowdown with a time sequence (10 min)*

Note: *OLGA* calculates itself the pressure in a flow line due to boundary conditions although there is no flow until 1200 second. This explains why the value of pressure during normal operation was not zero.

The pressures in 1^{st} stage and 2^{nd} stage separators can be observed from Figure 6.9. The black and dashed line is the pressure in 1^{st} stage separator, while the value of pressure in 2^{nd} stage separator is depicted by the red and solid line in the trend plot. The result is similar with the full blowdown case. At 1300 s, pressures in 1^{st} stage and 2^{nd} stage separators drop down to 13.43 *bara* and 12.07 *bara*, separately. When BDV2 opens at 1800 s, there is a decline again in the pressures. After BDV3 opens, the pressures 1^{st} stage and 2^{nd} stage separators reduce a little and retain around 12.80 *bara* and 12.06 *bara*, separately, during the rest of simulation time.

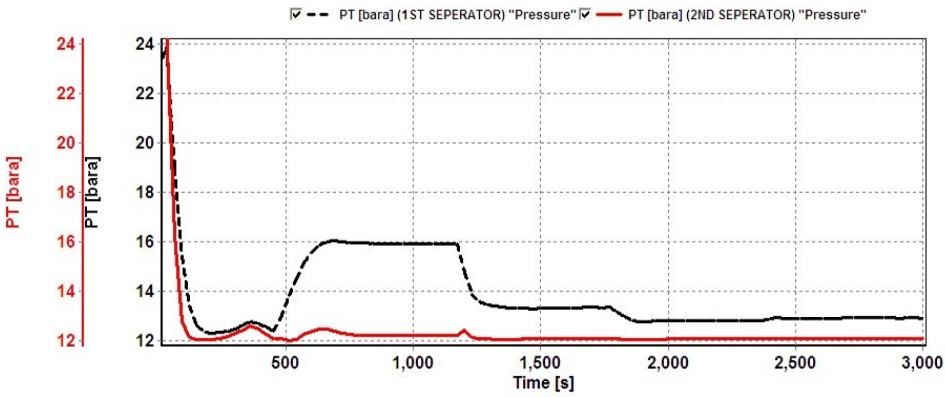

Figure. 6.9 *Pressure in 1^{st} stage and 2^{nd} stage separator during blowdown with a time sequence (10 min)*

6.7 Conclusions to Case Study 1

It is a clear presentation of transient process in flare line as well as in 1^{st} stage and 2^{nd} stage separators based on dynamic simulations in *OLGA* Flow Assurance. The study is carried out with two different cases, which are full blowdown and BDVs opening with a time sequence. The observation focuses on the mass flow rate and pressure in flare header, and pressures in 1^{st} stage and 2^{nd} stage separators. In accordance to the results, the intention is to find out the difference between full blowdown and BDVs opening in a series.

In terms of mass flow rate in flare line, the result does not show an evident advantage of blowdown with a time sequence. It is due to the limitations of simulated model because the dynamic model is lack of real data. At least, the mass flow rate is stepped up in Figure 6.7, while it rises up to a high value immediately after starting blowdown in the case of full blowdown. In addition, it is quite remarkable that the peak value in the case of blowdown with a time sequence is obviously lower than full blowdown. Based on this result, it emphasizes the benefit of adopting a time sequence to open BDVs comparing with full blowdown. By designing a proper opening sequence of BDVs, the maximum allowable operational condition in flare line can be ensured. Last but not least, both full blowdown and blowdown with a time sequence present a satisfied result in terms of the trend of pressures in 1^{st} stage and 2^{nd} stage separators, which means the pressure is reduced to a safe value within process safety time.

7 Case Study 2: Workability of Proposed Methodology

7.1 Introduction to Case Study 2

In order to demonstrate applicability of the suggested approach, a process consisting of a CSTR and cooling loop is considered. Liquid material A is feed into CSTR and liquid product B is taken out from outlet of CSTR. The reaction is exothermic. The cooling stream is injected by a cooling medium pump. The cooling stream will be stopped, if fault conditions appear in the cooling loop, such as leak in cooling loop. In addition, the CSTR is installed with three safety trips, Pressure Alarm High (PAHH), Level Alarm High High (LAHH) and Level Alarm Low Low (LALL), while the cooling system has a Pressure Alarm Low Low (PALL). The property and composition of the reaction are not described in detail.

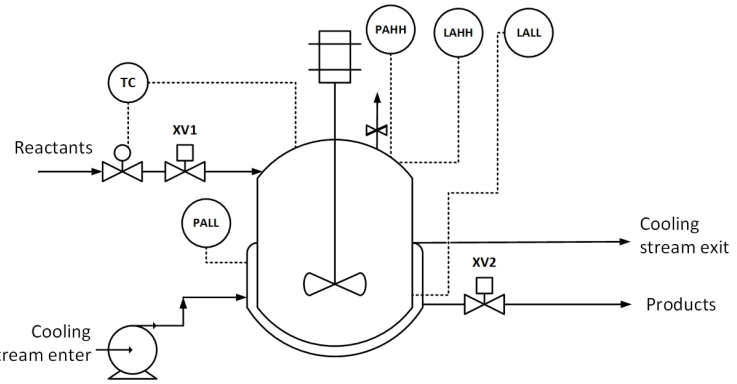

Figure. 7.1 *Information flow diagram of CSTR with a cooling loop*

In the system, there are two critical (shutdown) valves, XV1 and XV2, which is located at material inlet to CSTR and product outlet, separately. XV1 is final

element of PAHH and LAHH, while XV2 is automatically tripped if LALL in CSTR is initiated. When the pressure in cooling system is too low, the cooling medium pump will be automatically switched off. The information flow diagram of CSTR with a cooling loop is illustrated in Figure 7.1. In this case study, a dynamic model is established in Matlab.

7.2 Identification of Dangerous Combinations of Output States of SIS

Detailed information of methodology is introduced in Chapter 4. The analysis is essentially divided into three steps.

Step 1: Carry out system breakdown

Since the configuration of process is composed of a single piece of CSTR and cooling system, the work of first step in analysis can be omitted. The CSTR and cooling system are treated as a subsystem, which is considered in flowing steps.

Step 2: Identify dangerous combinations of safety trips

First of all, all the safety functions are clarified in the information flow diagram (see Figure 7.2). All possible combinations of simultaneously occurring safety trips are listed as follows:

- {PAHH in CSTR, LAHH in CSTR}
- {PAHH in CSTR, LALL in CSTR}
- {PAHH in CSTR, PALL in cooling system}
- {LAHH in CSTR, LALL in CSTR}
- {LAHH in CSTR, PALL in cooling system}
- {LALL in CSTR, PALL in CSTR}
- {PAHH, LAHH and LALL in CSTR}
- {PAHH and LAHH in CSTR, and PALL in cooling system}
- {PAHH and LALL in CSTR, and PALL in cooling system}
- {LAHH and LALL in CSTR, and PALL in cooling system}
- {PAHH, LAHH and LALL in CSTR, and PALL in cooling system}

Furthermore, the trips that have same final element should be removed from the list. Three safety functions, PAHH, LAHH and LALL, are installed in CSTR. Each function starts with the process sensor (e.g. PAHH, LAHH and LALL), and terminates with closing of the critical valve, XV1 or XV2. The final element of each safety function can be found in Table 7.1. Likewise, cooling system has a PALL, which is supposed to cut off the power supply of cooling medium pump in response to abnormal situation in cooling system. Table 7.1 presents the C&E diagram for the case study.

Table. 7.1 *C&E diagram for case study 2*

No.	Safety Functions	Process Unit	XV1	XV2	Switch off cooling medium pump
1	PAHH	CSTR	X		
2	LAHH	CSTR	X		
3	LALL	CSTR		X	
4	PALL	Cooling System			X

From Table 7.1, it shows that PAHH and LAHH in CSTR share a same final elements. In other words, these two trips have same effect on the process. Therefore, the combination of PAHH and LAHH in CSTR is not taken into further account. Consequently, the list of considerable combinations of safety trips is simplified as:

- {PAHH in CSTR, LALL in CSTR} ({1,3})
- {PAHH in CSTR, PALL in cooling system} ({1,4})
- {LAHH in CSTR, LALL in CSTR} ({2,3})
- {LAHH in CSTR, PALL in cooling system} ({2,4})
- {LALL in CSTR, PALL in cooling system} ({3,4})
- {PAHH and LALL in CSTR, and PALL in cooling system} ({1,3,4})
- {LAHH and LALL in CSTR, and PALL in cooling system} ({2,3,4})

For simplification, the safety trips are replaced with the number given in C&E diagram (Table 7.1).

For the pairs of safety trips that remain on the list, the next step is to check whether any of them may push the plant in direction of design limits. The worksheet is demonstrated in Table 7.2. LAHH and LALL can only happen at once, if two different instruments measuring the level and one of them has a spurious trip at the same time the other one trips due to an actual process condition. Thus, the probability of LAHH and LALL occurring concurrently in CSTR is extremely low. {2,3}and {2,3,4}can be directly removed from the list.

Table. 7.2 *Worksheet for identification of dangerous combinations of safety trips*

Subsystem	No.	Safety trips /installed location	Consequence	Dynamic Simulation
CSTR with cooling system	{1,3}	PAHH/CSTR + LALL/CSTR	• Reaction does not stop immediately due to residual materials. • Temperature in CSTR increases due to exothermic reaction. Cooling system keeps on functioning. • (**NOTE:** Cooling loop is often designed to sufficiently dissipate the heat generated by reaction during normal operation. Since PAHH is on demand, dynamic simulation is required to evaluate whether cooling loop can sufficiently dissipate the heat.)	
	{1,4}	PAHH/CSTR + PALL/cooling system	• No inflow. Product still comes out from outlet because of the materials remaining in reactor. • Temperature in CSTR increases due to exothermic reaction. Cooling system is lost.	
	{2,4}	LAHH/CSTR + PALL/cooling system	• Same as {1,4}	
	{3,4}	LALL/CSTR + PALL/cooling system	• Holdups in CSTR keeps on increasing since inflow continues entering into CSTR and outflow is terminated. • High temperature in CSTR due to exothermic reaction and loss of cooling system.	
	{1,3,4}	PAHH/CSTR + LALL/CSTR + PALL/cooling system	• Reaction does not stop immediately due to residual materials. • Temperature in CSTR rises up due to exothermic reaction and loss of cooling loop.	

If both materials and products are liquid state, PAHH also irregularly takes place with LALL at same time in CSTR. {1,3} and {1,3,4} can also be disregarded in this case. As a result, three scenarios are considered to perform dynamic simulations, involving {1,4}, {2,4} and {3,4}.

Step 3:Perform Dynamic Simulations.

In order to simulate the scenarios, dynamic models are established by using Matlab. The main idea is based on mole balance of reactant (A) and product (B) as well as energy balance of the system consisting of a CSTR with cooling system.

The reaction is single material A produces B. Both A and B are liquid state.

$$A \rightarrow B \tag{7.1}$$

There are two key assumptions for establishing the dynamic model and performing simulations.

1. There is no mixing volume, which means the holdups in reactor is only influenced by the quantities of inflow and outflow.
2. The density of inflow at inlet is same as the density of outflow at outlet of CSTR.

Mole balance:

$$\frac{dn_A}{dt} = F_{in} \cdot C_{A,in} - F_{out} \cdot C_{A,out} - r_A \cdot V \tag{7.2}$$

$$\frac{dn_B}{dt} = -F_{out} \cdot C_B + r_A \cdot V \tag{7.3}$$

Where

- F_{in}: Inlet flow rate
- F_{out}: Outlet flow rate
- $C_{A,in}$: Concentration of substance A at inlet
- $C_{A,out}$: Concentration of substance A at outlet
- r_A: Reaction rate of reactant A

The number of moles of substance A and B can be expressed as follows:

$$n_A = C_A \cdot V \tag{7.4}$$

$$n_B = C_B \cdot V \tag{7.5}$$

Where

- n_A and n_B: Number of moles of substance A and B, respectively
- C_A and C_B: Concentrations of substance A and B
- V: Component holdups of CSTR

The reaction rate can be expressed

$$r_A = k_A(T) \cdot C_A \tag{7.6}$$

The reaction rate constant can be written in accordance with Arrhenius equation.

$$k_A(T) = Ae^{-E/RT} \tag{7.7}$$

Where

- A: Pre-exponential factor or frequency factor
- E: Activation energy, J/mol
- R: Gas constant = 8.314 $J/mol * K$
- T: Absolute temperature, K

The values of parameter using in simulation can be found in Appendix B.

Energy balance:

An energy balance can be established for a non-isothermal CSTR in accordance to the first law of thermodynamics.

$$\left\{\begin{array}{c}Rate\ of\\ accumulation\\ of\ energy\\ within\\ the\ system\end{array}\right\} = \left\{\begin{array}{c}Rate\ of\\ energy\\ added\ to\ the\\ system\ by\\ mass\ flow\\ into\\ the\ system\end{array}\right\} - \left\{\begin{array}{c}Rate\ of\\ energy\\ leaving\\ system\ by\\ mass\ flow\\ out\ of\\ the\ system\end{array}\right\} + \left\{\begin{array}{c}Rate\ of\\ flow\ of\\ heat\ to\\ the\ system\\ from\ the\\ surrounding\end{array}\right\} - \left\{\begin{array}{c}Rate\ of\\ work\ done\\ by\ the\\ system\\ on\ the\\ surroundings\end{array}\right\} \tag{7.8}$$

Therefore,

$$\frac{dH}{dt} = F_{in} \cdot C_A \cdot h_A^0(T_0) - F_{out} \cdot C_A \cdot h_A(T) - F_{out} \cdot C_B \cdot h_B(T) + \Delta H(T)_{Rx} \cdot r_A \cdot V - \dot{Q} \tag{7.9}$$

Where

- $\frac{dH}{dt}$: Enthalpy changes per time unit
- $h_A^0(T_0)$: Enthalpy of substance A at initial temperature T_0
- $h_A(T)$ and $h_B(T)$: Enthalpy of substance A and B at temperature T
- $\Delta H(T)_{Rx}$: Reaction enthalpy at T
- $\dot{Q}$: Work done by cooling system for dissipating the heat generated by exothermic reaction.

It is assumed that $h_A^0(T_0)$ is zero. In addition, the enthalpy of substance A and B at temperature T can be given according to Kirchhoff's Law.

$$h_A(T) = C_{p,A} \cdot (T - T_0) \tag{7.10}$$

$$h_B(T) = C_{p,B} \cdot (T - T_0) \tag{7.11}$$

Where $C_{p,A}$ and $C_{p,B}$ stand for plasma concentrations of substance A and B.

Constitutive equations:

In conclusion, the dynamic models of system can be represented in the following condensed form:

$$\frac{dV}{dt} = F_{in} - F_{out} \tag{7.12}$$

$$\frac{dC_A}{dt} = \frac{F_{in}}{V} \cdot (C_{A0} - C_A) - r_A \tag{7.13}$$

$$\frac{dC_B}{dt} = \frac{F_{in}}{V} \cdot (-C_B) + r_A \tag{7.14}$$

$$\begin{aligned} \frac{dT}{dt} = & - \frac{F_{out} \cdot (C_A \cdot C_{p,A} \cdot (T - T_0) + C_B \cdot C_{p,B} \cdot (T - T_0))}{(C_A \cdot C_{p,A} + C_B \cdot C_{p,B}) \cdot V} \\ & + \frac{\Delta H(T)_{Rx} \cdot r_A \cdot V}{C_A \cdot C_{p,A} + C_B \cdot C_{p,B} \cdot V} - \frac{\dot{Q}}{C_A \cdot C_{p,A} + C_B \cdot C_{p,B} \cdot V} \end{aligned} \tag{7.15}$$

Matlab codes can be referred to Appendix B.

After building up a dynamic model, the scenarios that are confirmed in Step 2 can be simulated.

7.3 Results of Dynamic Simulation

The results of two scenarios are selected to be demonstrated. The two dangerous combinations are that LAHH in CSTR and PALL in cooling system occur at same time, and LALL in CSTR and PALL in cooling system occur at same time.

7.3.1 LAHH in CSTR and PALL in Cooling System

The initial states of triggering LAHH and switching off cooling medium pump are depicted in Table 7.3.

Table. 7.3 *Initial states of triggering LAHH and simulation time*

Holdups (L)	1600
$C_A(mol/L)$	1.2874
$C_B(mol/L)$	3.7152
$T(K)$	308.92
Simulation time (s)	150

The time point of triggering LAHH is treated as the start time of simulation. At time $t = 0$, XV1 is shut down and cooling medium pump is switched off. Figure 7.2-7.4 illustrate the outcomes of simulation.

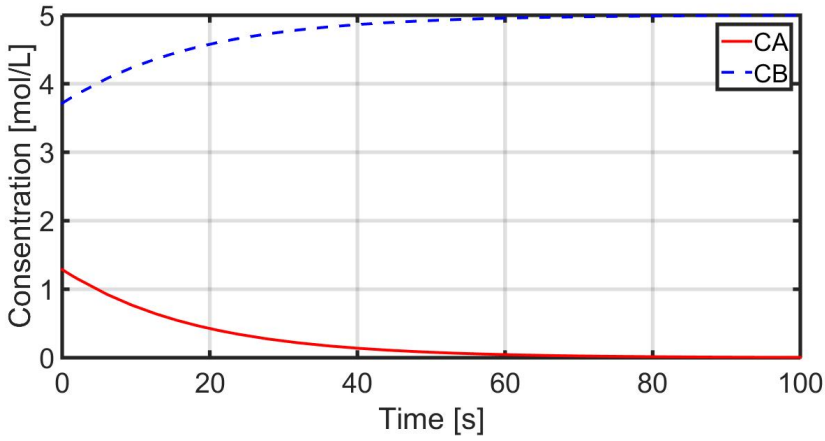

Figure. 7.2 *Development of concentrations of A and B versus time when LAHH in CSTR and loss of cooling occur concurrently*

Figure 7.2 presents how the concentrations of material A and product B change over the time, since inflow is shut down and cooling system is lost. While the red and solid line denotes concentration of material A, the concentration of product B is represented by the blue and dashed line. It can be seen that reaction continues producing B, even though the inflow has been stopped by tripping XV1.

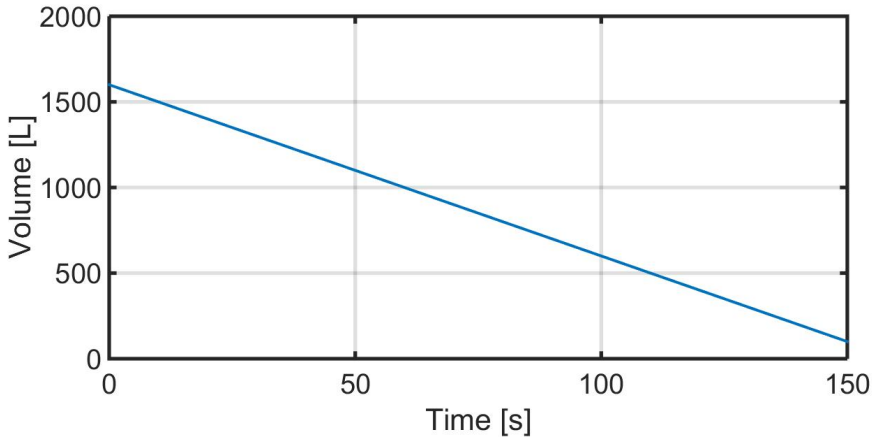

Figure. 7.3 *Development of component holdups versus time when LAHH in CSTR and loss of cooling occur concurrently*

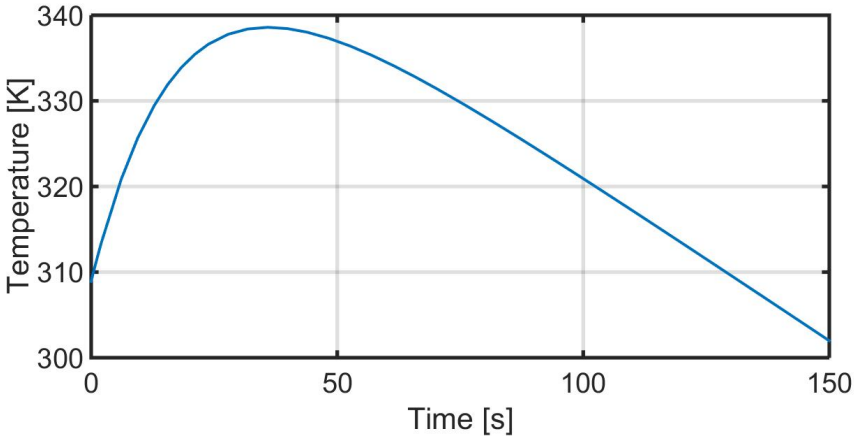

Figure. 7.4 *Development of temperature versus time when LAHH in CSTR and loss of cooling occur concurrently*

In Figure 7.3 and Figure 7.4, it indicates how the component holdups and temperature develop during the simulation time of 150 seconds. Component holdups

reduces due to no inflow. While, temperature increases from the beginning of simulation, and falls from 37 seconds. The peak value is approximately 339 K. The response of temperature is in agreement with the analysis in Step 2 (see Table 7.2). Since there are materials remaining in CSTR, temperature increases due to exothermic reaction and loss of cooling system. Since all materials are reacted, temperature starts to decrease. Dynamic simulation provides the information, such as how long the increase lasts, how much it increases, and when it turns to descend. After all, LAHH in CSTR and PALL in cooling system are activated at same time could be dangerous , since temperature in CSTR rises up to 339 K over a short period of time.

7.3.2 LALL in CSTR and PALL in Cooling System

The initial states of triggering LALL and switching off cooling medium pump are provided in Table 7.4.

Table. 7.4 *Initial states of triggering LAHH and simulation time*

Holdups (L)	400
$C_A(mol/L)$	0.8874
$C_B(mol/L)$	4.7152
$T(K)$	300.92
Simulation time (s)	150

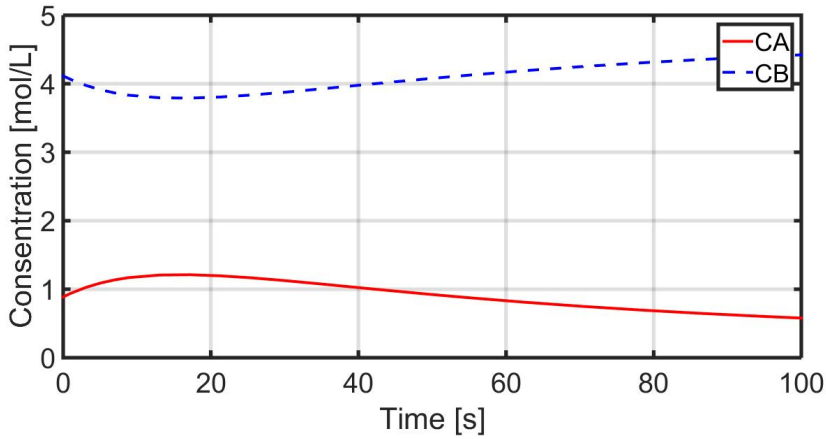

Figure. 7.5 *Development of concentrations of A and B versus time when LALL in CSTR and loss of cooling occur concurrently*

The time point of initiating LALL is treated as the start time of simulation. At time $t = 0$, XV2 is shut down and cooling medium pump is switched off. Figure 7.5-7.6 portray the results of simulation. Figure 7.5 describes how the concentrations of material A and product B vary over the time, while LALL in CSTR and PALL in cooling system occur concurrently. During the first 20 seconds, the concentration of material A ascends, since the outflow is stopped by closing XV2 and product B is remained in CSTR. Afterwards, it gradually rises up because inflow continues entering into CSTR and the flow rate is higher than the reaction rate.

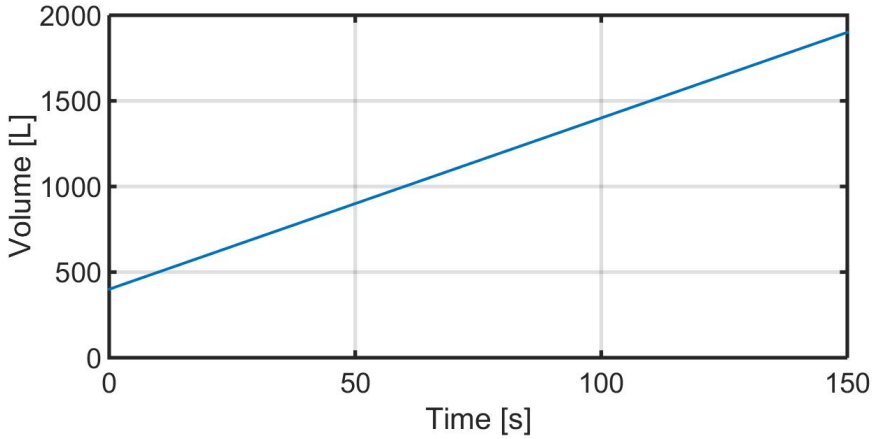

Figure. 7.6 *Development of component holdups versus time when LALL in CSTR and loss of cooling occur concurrently*

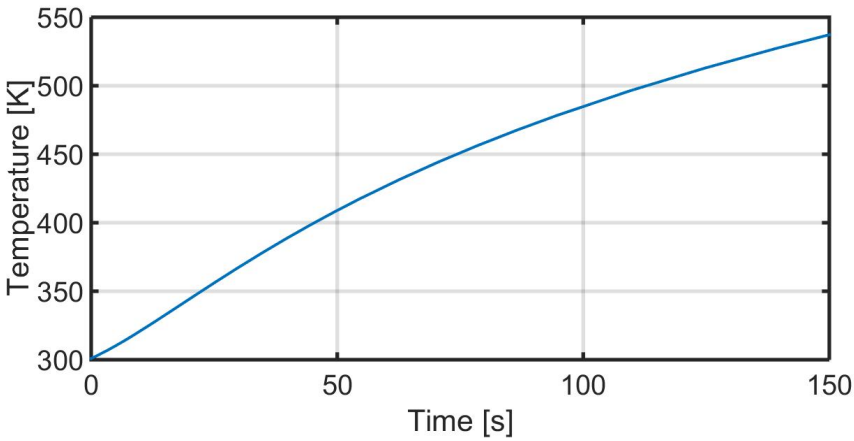

Figure. 7.7 *Development of temperature versus time when LALL in CSTR and loss of cooling occur concurrently*

In Figure 7.6 and Figure 7.7, it shows how the component holdups and temperature develop during the simulation time of 150 seconds. Different from the results of the first scenario, both component holdups and temperature experience dramatic increase over the period of simulation time because the inflow continues entering in CSTR, the outflow is terminated and cooling system is lost. Therefore, LALL in CSTR and PALL in cooling system activating at same time can lead to a extremely dangerous situation.

7.4 Conclusions to Case Study 2

Although the case study is based on a process with a simple configuration, it is enough to show workability of proposed methodology (in Chapter 4). In accordance with the three steps and the scope of analysis, three dangerous combinations of simultaneous occurring safety trips were confirmed as scenarios of dynamic simulation, including combinations of PAHH in CSTR and PALL in cooling system, LAHH in CSTR and PALL in cooling system, and LALL in CSTR and PALL in cooling system. Results from dynamic simulations show that it can be dangerous if several safety instrumented functions occur concurrently. In particular, LALL in CSTR and PALL in cooling system are on demand at same time. The situation can be very dangerous without further protection measures. In other words, the dangerous combinations should be paid enough attention during process design.

A worksheet (see Table 7.2) is made during the analysis. The worksheet together with a report containing the results of simulation scenarios should be made for inclusion in the safety requirements specification of SIS. A formal worksheet for identification of dangerous combinations of output states of SIS is attached in Appendix A. Probability assessment is not executed in the case study with the purpose to focus on demonstrating the result of dynamic simulation. For a real practice of the methodology, it should not be omitted.

8 Conclusions, Discussions and Recommendations for Future Work

8.1 Conclusions

SIF is implemented by a SIS and given a specific safety integrity level. The safety, however, should be considered with a comprehensive perspective. It is inevitable to ensure the risk reduction measures do not result in a new hazard event in process or plant. IEC61511 [2] requires identifying dangerous combinations of output states of SIS. However, the effect of an individual safety trips on system level is always overlooked in SIS design. Although SIS functions as expected, simultaneously occurring safety trips may generate a hazard event because of interactions between different process units. Variability also goes through and oscillates entire process via recycled loops.

Modification of blowdown and flare system on topside platform is a practical example to emphasize the essential of considering global effect on system level. BD valves are organically installed to protect a single process unit, i.e. separators and pipeline, after shutdown. Process intensification is also considered as inherently safer design. Due to increasing number of tie-in subsea wells, a full blowdown may exceed the design limits of a designed flare header. Replacing a flare header is always too expensive to invest. An alternative solution of avoiding overcapacity is to design a proper time sequence of BD valves opening time. It is necessary to perform dynamic simulations for different combinations of BD valve opening.

HAZOP study is a common approach for hazard identification in process industry. However, the drawbacks of the method make it inadequate to uncover hazard event due to simultaneously occurring safety trips. In accordance with safety lifecycle model in IEC61511 [2], "hazard and risk assessment" and "allocation of safety functions to protection layers" are two critical phases, which give input to SRS. A literature review is done with respect to various hazard identification methods. There are a number of approaches available for hazard analysis, including checklists,

what-if analysis, FMEA, HAZOP study, cause and consequence analysis, HAZOP log, Change analysis, Maser diagram and so on. Each of the methods has their own pros and cons. It is an interesting finding that some techniques are particularly utilised in certain stages of a lifecycle for process hazard studies. Unfortunately, none of them is able to identify dangerous combinations of output states of SIS, which created the need of a methodology that can serve the purpose and fulfil the requirements in IEC61511 [2].

Targeting at identifying a sort of new hazard event, a three-step method is proposed. It is new hazard event because hazard event occurs with SIS functioning in demand mode. The main idea of the method is to break down the system, identify dangerous combinations of safety trips and perform dynamic simulations. Based on information flow diagram, the system is initially broken down into subsystems, which can be analysed individually. The inspiration of algorithm is based on the Sargent-Westergerg algorithm. In order to accomplish the analysis, a vital assumption is that the new hazard event resulting from simultaneously occurring safety trips is only considered when a same time-scale is utilized for determining the leading effects on process or plant. There are also three rules for developing the list of subsystems. Within each subsystem, the second step is to select the combinations of safety trip, which may yield a response that pushes the plant towards its design limits. It can be achieved by using an analysis that is similar with conventional HAZOP study. With regard to combinations of safety trips, the question is "Could it cause high pressure?" "Could it cause low pressure?" and so on. From the worksheet, a list of scenarios for dynamic simulation should be confirmed. The last step, performing dynamic simulation, should be able to answer whether the combination of simultaneously occurring safety trips violate the design limits of process or plant. There are varieties of different solution tools, which can be applied to perform dynamic simulation.

In the three-step method of identification of dangerous combinations of output states of SIS, probability is also taken into account. The risk can be treated as acceptable, if the probability of the occurrence of simultaneously occurring safety trips is too low. Common cause failure may significantly increase the demand rate. If the probability is unneglectable, it is necessary to perform dynamic simulations and to propose design mitigation action as well.

The first case study is multiple releases to a flare header on topside platform. The use of blowdown and flare system as a case study is to demonstrate the transient process of simultaneous occurring safety trips in an interconnected flow network. A dynamic model is established in a specialized dynamic process modelling software, *OLGA* Flow Assurance. The observation is mainly based on a comparison between full blowdown and opening BD valves in a time sequence. Because of increasing number of tie-in subsea wells, a scenario of full blowdown (opening all BD valves at once) may exceed the design limits of flare header. The outcome of case study 1 confirms that a proper time sequence to open BD valves is helpful to prevent overcapacity.

Furthermore, case study 2 is a chemical process comprising a CSTR and cooling system. Several PSD functions are installed in system, including PAHH, LAHH and LALL in CSTR, and PALL in cooling system. Although the case study is based on a process with a simple configuration, it is enough to show workability of proposed methodology (in Chapter 4). Matlab is used to build up a dynamic model. In accordance with three-step method, three dangerous combinations of simultaneous occurring safety trips are confirmed as scenarios of dynamic simulation, involving combinations of PAHH in CSTR and PALL in cooling system, LAHH in CSTR and PALL in cooling system, and LALL in CSTR and PALL in cooling system. Results from simulation scenarios show that it can be dangerous if several safety instrumented functions occur concurrently. If LALL in CSTR and PALL in cooling system are on demand at same time, the situation can be very dangerous without further protection measures. Probability assessment is omitted in the case study with the purpose to focus on dynamic simulation and to illustrate the results. The outcome of case study 2 reveals the essential of evaluation of output states of SIS and confirm the applicability of the proposed method.

8.2 Discussions

When SIS is designed in a local system, the effect on global system level cannot be ignored. In striving to fulfil the requirements of identification of dangerous combinations of output states of SIS in IEC61511 [2], a generic method is proposed. In accordance to safety lifecycle model, all potential hazards are necessarily identified in the phase of hazard and risk assessment. However, there are several stages of hazard analysis during a project development. A proper time schedule for carrying out an analysis based on suggested method is of interest. As mentioned in the description of the approach, it should be based on information flow diagrams. Moreover, NOG070 [5] Annex E provides the information that the identification of dangerous combination of outputs of SIS should be included in the SRS rev.3 , which is after overall safety validation planning. According to the diagram, the SRV rev. 3[1] is developed based on the final SAR (safety analysis report), when detailed drawing is available from SIS vendors.

The advantages of the method is that it is based on engineer experience to obtain the list of scenarios for dynamic simulation. Complex system is divided into subsystems, which can be effectively handled and individually analysed. In addition, dynamic simulations can capture transient process. There are plenty of solution tools available to perform dynamic simulations. On the other hand, the analysis can be time consuming for a complicated system with many safety functions. Dynamic simulation requires specific skills and knowledge. Other advantages and weaknesses regarding suggested method may be realized, when the method is put

[1]SRS is not only a design-related document, but a document that must remain updated throughout the whole life cycle of the SIS. A SRS time axis is suggested in NOG 070 [5] Annex -E, where the relevant SRS revision are defined in the chronological order or events.

into practice.

The progress of technology, such as new materials and new equipment, enables process industry to expect a new economic target. Tie-in project in offshore Oil & Gas industry is a typical example. Moreover, it is also tendency of applying highly integrated system for instance in fine chemical industries with major purpose to save energy. The key point is that it brings challenges to process control system design due to increased complexity of production/processing system or new economic objective. The safety should be considered with a comprehensive analysis.

8.3 Recommendations for Future Work

The limitation of this master thesis is lack of real project data. Future research work is encouraged to put suggested approach into practice and to test the approach with a complex process system. Dynamic models in two case studies were established in *OLGA* Flow Assurance and Matlab, while there are many different solution tools available for dynamic simulation. The applicability of method can also be demonstrated with other dynamic simulators.

The master thesis is targeted at an interdisciplinary topic. Researchers in the field of process control and optimization can further develop and improve the technique of identification of dangerous combinations of output states of SIS. In addition, it can be a valuable research direction, which considers the safety issues of implementing SIS in a process system.

Bibliography

[1] *IEC 61508. Functional Safety of Eletronical/Eletronic/Programmable Eletronic Safety-related Systems.* International Eletrotechnical Commission, 2010.

[2] *IEC61511. Functional Safety-Safety Instrumented Systems For the Process Industry Sector.* International Eletronical Commission, 2003.

[3] D. E. Seborg, T. F. Edgar, and D. A. Mellichamp, *Process, Dynamics and Controls.* United States: John Wiley & Sons, Inc., 2003.

[4] B. Schrors, "Functional safety: Iec61511 and the industrial implementation," 2010.

[5] *OLF-070. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.* The Norwegian Oil Industry Association, 2004.

[6] M. Rausand, *Risk Assessment: Theory, Method and application.* United States: Wiley, 2011.

[7] *IEC61882 Hazard and Operability Studies (HAZOP studies) -Application Guide.* International Eletrotechnical Commission, 2001.

[8] T. Lasson and S. Skogestad, "Plantwide control - a review amd a new design procedure," *Modeling, Identification and Control*, pp. 209–240, 2000.

[9] *Guidelines for Hazard Evaluation Procedures.* CCPS, 2008.

[10] W. V. Wassenhove, *Chapter 15 Dynamic Simulation of Gas Processing Plants.* Elsevier Inc., 2015, pp. 467–485.

[11] *ISO10418 Petroleum and natural gas industries offshore production installations basic surface process safety systems.* The international Organization for Standarization, 2003.

[12] W. L. Luyven, B. D. Tyreus, and M. L. Luyben, *Plantwide process control.* New York: MacGraw-Hill, 1998.

[13] M. Rausand and A. Hoyland, *System Reliability Theory: Models, Statistical Methods, and Applications Second Edition.* New Jersey: John Wiley & Sons, 2004.

[14] M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications.* New Jersey: John Wiley & Sons, Inc., 2014.

[15] S. Hauge, T. Krakenes, S. Habrekke, and H. Jin, *Reliability Prediction Method for Safety Instrumented System.* SINTEF Technology and Society, 2013.

[16] H. Jin, M. A. Lundteigen, and M. Rausand, "Reliability performance of safety instrumented systems: a common approach for both low- and high-demand mode of operation," *Reliability Engineering and System Safety*, pp. 365–373, 2011.

[17] T. A. Kletz, "Looking beyond alarp overcoming its limitations," *Process Safety and Environmental Protection*, vol. 83, no. B2, pp. 81–84, 2005.

[18] J. C. Etchells, "Process intensification safety pros and cons," *Process Safety and Environmental Protection*, vol. 83, pp. 85–89, 2005.

[19] D. Macdonald, *Practical Industrial Safety, Risk Assessment and Shutdown Systems.* Burington: Newnes, 2004.

[20] B. Hekkelstrand and P. Skulstad, *Guidelines for the protection of pressurised systems exposed to fire.* Scandpower Risk Management Ltd., 2004.

[21] *NORSOK S-001 Technical Safety.* Standards Norway, 2008.

[22] *Subsea Facilities - Technology Developments, Incidents and Future Trends.* DNV GL, 2014.

[23] S. Hauge, P. Hokstad, and T. Onshus, "The introduction of iec61511 in norwegian offshore industry."

[24] N. Ramzan, F. Compart, and W. Witt, "Application of extended hazop and event-tree analysis for investigation operational failures and safety optimization of distillation column unit," *Process Safety Progress*, pp. 248–257, 2007.

[25] CCPS, *Layer of protection analysis-simplified process risk assessment.* Centre for Chemical Process Safety (CCPS), 2001.

[26] J. Dunjo, V. Fthenakis, J. A. Vilchez, and J. Arnaldos, "Hazard and operability analysis. a literature review." *Journal of Hazard Materials*, p. 19/32, 2010.

[27] N. Razmzan, F. Compart, and W. Witt, "Methodology for the generation and evaluation of safety system alternatives based on extended hazop," *Process Safety Progress*, pp. 35–42, 2007.

[28] L. Christopher A., "Layer of protection analysis (lopa) for determination of safety integrity level," 2008.

[29] T. Gundersen and T. Hertzberg, "Partitioning and tearing of networks-applied to process flowsheeting," *Model, Identification and Control*, pp. 139–165, 1983.

[30] R. W. H. Sargent and R. B. Westerberg, "Speedup in chemical engineering design," *Trans. Inst. Chem. Eng*, pp. 190–197, 1964.

[31] *API RP-14C Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms.* API Publishing Service, 2007.

[32] H. S. Fogler, *Essentials of Chemical Reaction Engineering.* Prentice Hall, 2011.

[33] A. C. Dimian, C. S. Bildea, and A. A. Kiss, *Chapter 4 Dynamic Simulation.* Elsevier B. V., 2014, pp. 127–156.

[34] M. Hillestad and T. Hertzberg, "Dynamic simulation of chemical engineering systems by the sequential modular approach," *Computers & Chemical Engineering*, vol. 10, no. 4, pp. 377–388—, 1986.

[35] *NORSOK Standard P-100 Process Systems.* Standards Norway, 2001.

[36] T. Brzustowski, "Flaring in the energy industry," *Progress in Energy and Combustion Science*, vol. 2, no. 3, pp. 129–141, 1976.

[37] *NORSOK Standard P-001 Process Design.* Standards Norway, 2008.

[38] R.-E. Meidndinyo T., "Thermo-hydraulic modeling of flow in flare systems," 2012.

[39] H. Raddum, "Dynamic modelling and simulation of flare systems," Conference Proceedings.

A Worksheet for Identification of Dangerous Combinations of Output States of SIS

System Name

Reference Date

Subsystem	No.	Safety trips/Installed location	Consequence	Dynamic simulation	Responsible	Comment
CSTR with cooling system	{2,4}	LAHH/CSTR + PALL/cooling system	No inflow. Product still comes out from outlet because of the materials remaining in reactor. Temperature in CSTR increases due to exothermic reaction. Cooling system is lost.	X		

B Matlab Codes

```
function dx = cstr1(t,x,u)

% states
V = x(1);
CA = x(2);
CB = x(3);
T = x(4);

%Model parameters
CA0=5;
kA = 0.08;
EA = 1000;
R = 8.314;
T0 = 298.15;
CpA = 25;
CpB = 30;
HRX = 5000;

% Kinetic model
RA=@(T,CA)kA*exp(-EA/(R*T))*CA;

%Input signal

Fin = u(1);

Fout = u(2);

Q = u(3);

%State derivatives

dV = Fin - Fout;

dCA = (Fin/V)*(CA0-CA)-RA(T,CA);

dCB = (Fin/V)*(-CB)+RA(T,CA);

tc = V* (CpA*CA+CpB*CB);

dT = -Fout*(CA*CpA*(T-T0)+CB*CpB*(T-T0))/tc+HRX*RA(T,CA)*V/tc-Q/tc;

dx = [dV, dCA, dCB, dT]';
end
```

C FMEA Worksheet

Description of unit			Description of failure			Effect of failure		Risk				Risk reducing measure	Respons ible	Comment
Ref. no.	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the sub-system	On the system function	Fre.	Sev.	Detecta bility	RPN			
4.1	Close gas flow	Normal operation	-Valve fails to close on demand	-Spring broken -Hydrates in valve -Too high friction in actuator	Periodic function test	Shutdown function failed	Production must be stopped	2	4	4	10	Periodic control of spring Periodic operation of valve		
			-Leakage through the valve.	-Erosion in valve seat -Sand between valve seat and gate	Periodic function test	Shutdown function degraded	System must be repaired within one month	2	3	5	10	Improved startup control to prevent sand production		
4.2	Open gas flow	Closed	Valve cannot be opened on command	-Leakage in hydraulic system -Too high frication in actuator	Immediately detected	Cannot start production	System cannot produce							