Title: Utilization of Risk Priority Number to Systems-Theoretic Process Analysis: A Practical Solution to Manage a Large Number of Unsafe Control Actions and Loss Scenarios

Hyungju Kim*, Mary Ann Lundteigen (mary.a.lundteigen@ntnu.no) **, Andreas Hafver***, Frank Børre Pedersen***

* University of South-Eastern Norway (USN)

** Norwegian University of Science and Technology (NTNU)

*** DNV-GL

Abstract

System-Theoretic Process Analysis (STPA) is a relatively new hazard identification method whose main assumption is that accidents can be caused by unsafe interactions of system components, as well as component failures. STPA can cover a wider range of hazards compared with traditional hazard analysis methods, such as software flaws, human errors, component failures, and complex interactions of system components. Identifying more hazards is of course an important advantage of STPA, but generating too many hazards may pose a practical challenge to stakeholders to utilize the results of STPA.

Some hazards or scenarios may be more critical with higher consequence, while others can be less critical with lower consequence. We therefore need to evaluate the analysis results to focus on more critical and important problems first, especially when we do not have enough time and resources to solve every problem identified by the analysis. The main objective of this study has been to suggest an additional procedure to STPA to ensure a systematic evaluation, screening and prioritization of analysis results.

The risk priority number (RPN) approach was adopted to evaluate the criticality of the results of analyses. After investigating the strengths and limitations of traditional RPN approaches, three new RPN criteria along with four additional procedure steps were added to the STPA for evaluation, screening and prioritization of STPA results. The proposed criteria and procedure have been demonstrated with a case study of a subsea gas compression system, and for this particular analysis, it was suggested that 38 out of 130 UCAs and 258 out of 976 loss scenarios were significantly less critical and screened out, so that the resources could be prioritized to solve the remaining findings. At the same time, prioritization is still a rather new topic with STPA, and in the end of the paper, we have identified some ideas for further research in this area.

1. Introduction

System-Theoretic Process Analysis (STPA) is a relatively new hazard identification method that is based on the System-Theoretic Accident Model and Processes (STAMP) [1]. In STAMP, conception of causality of accidents is not limited to component failures, but extended to include component interaction accidents [2]. STPA therefore assumes that accidents can be caused by unsafe interactions of system components, as well as component failures [1]. STPA introduces two key concepts in relation to the hazards identification: (1) unsafe control actions (UCAs), which cover wrong or lack of adequate appliance of control commands that can result in accidents or losses of vital system functions, and (2) loss scenarios, which describes the causal factors that can lead to the UCAs and to hazards [1].

One advantage of STPA that is advocated in the literature [2] is the ability to cover a wider scope of hazards than traditional hazard identification methods, such as fault tree analysis (FTA), and failure modes, effects, and criticality analysis (FMECA). Many studies have demonstrated that STPA can identify not only all causal scenarios found by traditional methods, but also a large number of additional software-related and non-failure scenarios that were not identified by the traditional methods [1]. For instance, Fleming, Spencer [3] and Ishimatsu, Leveson [4] applied STPA to a flight control system and unmanned spacecraft respectively, and compared the results with FTA. Abrecht [5] analyzed an offshore supply vessel dynamic positioning system using STPA, and compared STPA with FTA and FMEA. Pawlicki, Samost [6] applied STPA to health care with comparisons with FMECA. Sotomayor Martínez [7] and Abrecht, Arterburn [8] analyzed automotive applications and rotorcraft respectively, and compared the results with FMEA. In these studies, STPA could identify additional loss scenarios that could not have been found by traditional hazard identification methods.

As a result of this advantage, STPA necessarily produces a higher number of loss scenarios than traditional methods. A detailed STPA may in turn also identify hundreds of unsafe control actions (UCAs) and thousands of loss scenarios. Unlike other traditional methods, STPA does not include any evaluation process for the identified UCAs and loss scenarios, because Leveson and Thomas [1] argue that probability or likelihood of the loss scenarios cannot be known in early design stage, or if the system is software-intensive, or when the system differs significantly from past systems. Evaluating UCAs and loss scenarios with numbers that do not accurately reflect the risk can dangerously mislead us into dismissal of critical scenarios [9].

One practical problem originates from these two characteristics of STPA: (1) a higher number of UCAs and loss scenarios and (2) no evaluation of them. It might be inefficient to manage a large number of UCAs and scenarios without evaluating criticality, because some UCAs and scenarios can be highly critical and lead to severe losses, while others can be less critical and lead to minor losses. Hafver, Eldevik [10], Kim, Lundteigen [11] and Zikrullah [12] have also recognized the need to evaluate the results of STPA to help focus our efforts to improve safety.

The main objectives of this paper are: (1) to emphasize the necessity for evaluation of STPA results, including screening and prioritization, to manage a large number of UCAs and loss scenarios, (2) to suggest additional procedures for the evaluation, and (3) to demonstrate the new procedure with a case study. For this purpose, the remaining part of this paper is organized as follows: STAMP and STPA are briefly introduced in Section 2, and the practical challenges of STPA to manage a large number of UCAs

and loss scenarios are discussed in Section 3. A solution for these challenges is proposed in Section 4, and the solution is demonstrated in Section 5. Results and discussions are presented in Section 6, which is followed by concluding remarks in Section 7.

2. Introduction to STAMP and STPA

2.1. STAMP, STPA and CAST

STAMP was first introduced by Leveson [2]. The motivation for introducing STAMP as a framework was the need for a new approach to build safer systems, because significant changes have occurred in modern systems. Challenges faced include the fast pace of technological change, reduced ability to learn from experience, changing nature of accidents, new types of hazards, increasing complexity and coupling, decreasing tolerance for single accidents, difficulty in selecting priorities and making tradeoffs, more complex relationships between humans and automation, changing regulatory, and public views of safety. With basis in these significant changes, Leveson introduced new theses about safety and why accidents occur, whose main philosophy is that accidents occur not because of failure problems but due to inadequate control problems, and she developed an expanded accident causality model, called System-Theoretic Accident Model and Processes (STAMP). STAMP expands the accident causality model from a chain of directly related failure events or component failures, to complex and unsafe interactions among system components. Therefore, STAMP does not treat safety as a failure prevention problem, but as a dynamic control problem, including component failures as a subset [1].

Two analysis techniques were introduced based on the STAMP model: System-Theoretic Process Analysis (STPA), and Causal Analysis based on Systems Theory (CAST) [1]. STPA is a hazard identification method that proactively analyzes potential causes of accidents, while CAST is an accident/incident investigation method that retroactively identifies the causal factors of accidents. The relationship among STAMP, STPA and CAST is illustrated in Figure 1. The main focus in this paper has been on the use of STPA to support decision-making in design of new systems.

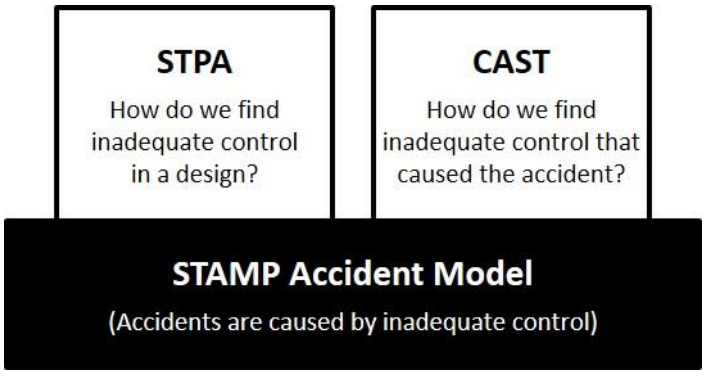

Figure 1 Relationship among STAMP, STPA and CAST [13]

2.2 System-Theoretic Process Analysis (STPA)

The main assumption of STPA is that any loss associated with the dysfunction of a system can be caused by improper interactions of system components, with or without individual component failures [1]. The losses can be related to human damages, environmental damages, or loss of critical services and assets. The aim of STPA is to study all functions, including those provided by controllers, sensors, actuating devices, and by human interaction. This means that hazards (in the sense that they can lead to losses) related to design errors, software flaws, component interactions, complex human decision-making errors, and social, organizational, and management factors contributing to accidents are within the scope of STPA [2].

The STPA Handbook [1] introduces four steps of the STPA method: (1) define purpose of the analysis, (2) model the control structure, (3) identify unsafe control actions, and (4) identify loss scenarios. An overview of the main steps is shown in Figure 2.

The first step is, like in any analysis method, to define the purpose of the analysis, including fundamental questions about scope of losses and defining the system boundary. It consists of four sub-steps: (a) identify losses, (b) identify system-level hazards, (c) identify system-level safety constraints, and (d) refine hazards (optional). The outputs of this step are lists of losses, system-level hazards, system-level safety constraints, and refined hazards. The second step is to build a control structure model of the system that captures functional relationships and interactions, by identifying responsibilities, process models and feedbacks. For this step, we (a) establish an abstract control structure, (b) identify responsibilities, process models and feedbacks of each controller, and (c) refine the control structure with process models and feedbacks. The output of this step is a control loop diagram with responsibilities of controllers and associated feedbacks. The third step is to investigate control actions in the control structure and identify unsafe control actions that can lead to the losses defined in the first step. This step consists of: (a) examine combinations of control actions and process models, (b) identify UCAs, and (c) identify controller constraints. The outputs are lists of UCAs and associated controller constraints. The last step is to investigate why and how unsafe control actions identified in the third step occur in the system. Two kinds of scenarios are identified in this step: scenarios that lead to UCAs and scenarios in which control actions are improperly executed or not executed. The outcome of this step is a list of loss scenarios. The results of STPA can be utilized for generation of system test and evaluation requirements, control of manufacturing, and generation of operational safety requirements. For more details of the STPA procedure, the reader can refer to the STPA Handbook [1].

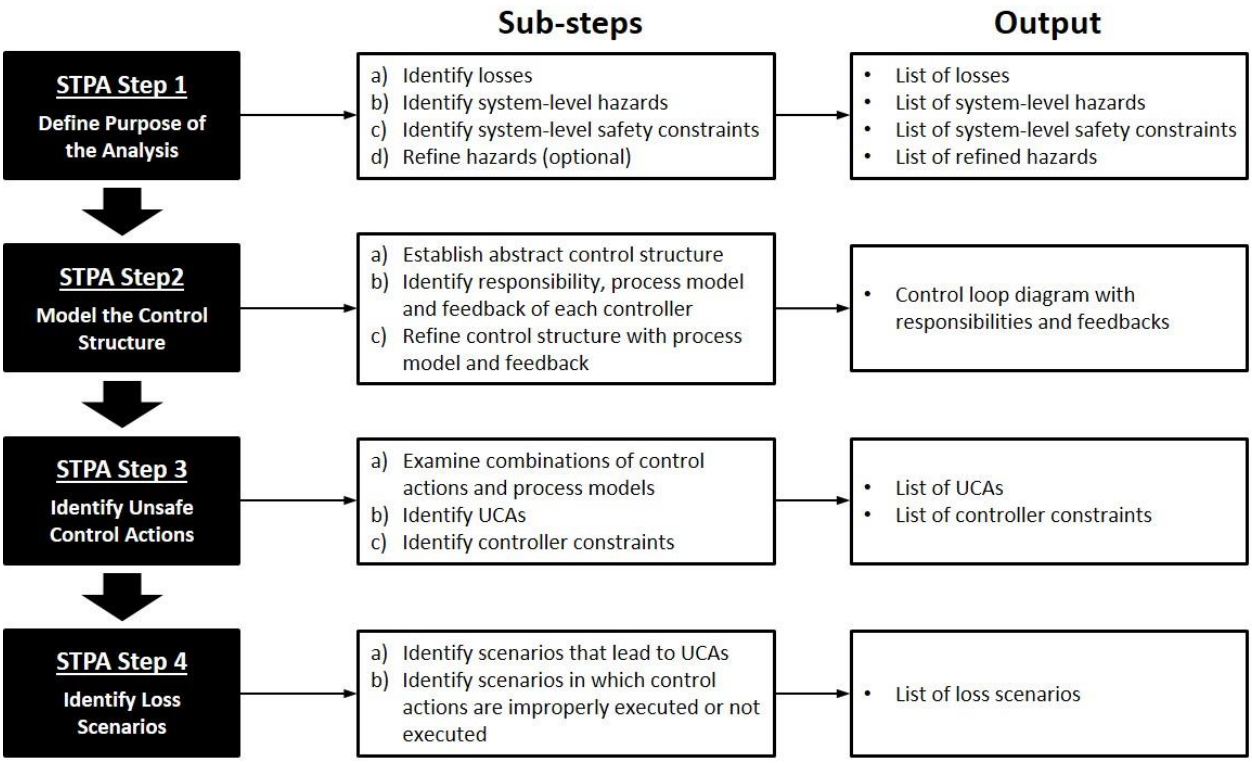

Figure 2 STPA procedure and output

Many studies have showed that STPA can identify additional casual scenarios that are not easily found by traditional methods, as well as all the causal scenarios found by the traditional methods [1]. Another advantage is that STPA is a top-down approach. STPA can be applied from an early stage of project development to identify design flaws, so that costly rework caused by design flaws identified too late can be eliminated [1]. STPA is therefore widely used in various sectors and domains, like aviation [14], aerospace [15], healthcare [16], maritime [17], oil and gas [18], and so on.

3. The Challenge of Managing a Large Number of UCAs and Loss Scenarios

While the results of an STPA typically include hundreds of UCAs and thousands of loss scenarios, STPA has neither a procedure to prioritize important hazards, nor to screen out minor hazards. The designers or stakeholders are therefore led to treat all the UCAs and loss scenarios equally, regardless their criticality. This may be inefficient use of resources, as a significant amount of efforts may be spent on solving less important problems. For instance, suppose we identified 1,000 loss scenarios from a system, and 10 of them are highly critical, while the other scenarios are less critical with minor consequence. If we do not evaluate criticality of each scenario and treat them equally, we may use 99% of our resources to solve less critical problems, and only 1% of our effort can be allocated to solve highly critical problems. In the worst case, if we do not have enough time and resources to solve every problem identified by STPA, we may spend all of our time and resources to solve less critical problems, and the 10 critical problems may be left unsolved, although they might have been easy to fix. A challenge of STPA in practical application is therefore to

"Manage a large number of unevaluated UCAs and loss scenarios"

We acknowledge that assigning probabilities or likelihood to human errors and software flaws poses a practical challenge [8], and this can mislead us into dismissal of important causal factors [9]. However, not evaluating UCAs and loss scenarios can also lead to another kind of problem mentioned above. Evaluation of STPA results is necessary to allow optimal allocation of resources to improve the safety [10, 11].

To explore this challenge in detail, this paper utilizes a case study that applies STPA to a subsea gas compression system [11]. The subsea gas compression system separates and boosts gas and liquid from the seabed to the offshore platform on the sea, and the system consists of a scrubber, a gas compressor with variable speed drive (VSD), flow/temperature/pressure transmitters, a liquid discharge valve, an anti-surge valve, and shutdown valves. The liquid discharge valve controls the liquid level inside the scrubber, so the liquid will not flow into the gas compressor. The anti-surge valve controls the pressure at the outlet of the compressor to prevent surge, and the shutdown valves isolate the subsea compressor system in case of an emergency.

Four losses in Subsea Gas Compression (SGC) were identified: loss of life or injury to people, environmental pollution, damage to valuable subsea equipment, and reduced gas production. Related system-level hazards and system-level constraints are listed in Table 1, and a control loop diagram is shown in Figure 3

Table 1 Losses, system-level hazards and constraints of subsea gas compression system[11]

System	Losses	System-Level Hazards	System-Level Constraints
Subsea Gas Compression System	L-1: Loss of life or injury to people	H-1: SGC system continues to supply gas when gas leaks to the environment	SC-1: SGC system must stop compressing gas when gas leaks to the environment
	L-2: Environmental pollution		
	L-3: Damage to valuable equipment	H-2: SGC system operates under abnormal conditions	SC-2: SGC system must be protected from abnormal operating conditions that can damage valuable equipment
	L-4: Reduced gas production	H-3: SGC stops operation unnecessarily or SGC setpoints are not optimal	SC-3: SGC system must never stop unnecessarily and SGC setpoints must always be optimal

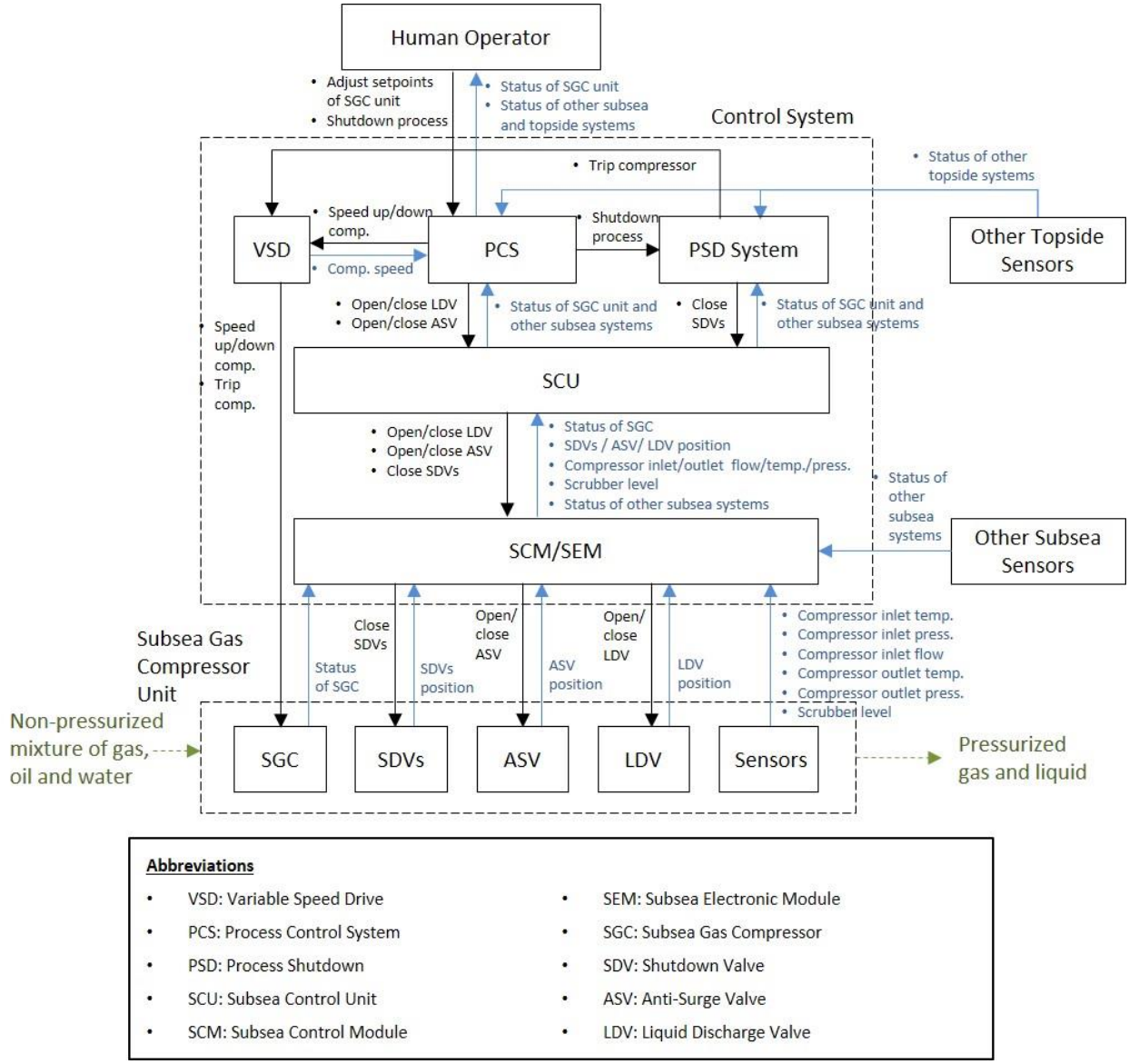

Figure 3 Control loop diagram of subsea gas compression system[11]

From the control structure depicted in Figure 3, 130 UCAs and 976 loss scenarios were identified. Among the 130 UCAs, 18 UCAs were related to H-1 in Table 1, 55 UCAs to H-2, and 57 UCAs to H-3. 160 loss scenarios out of 976 were connected to H-1, 416 loss scenarios to H-2, and 400 loss scenarios to H-3. The number of UCAs and loss scenarios with related system-level hazards are presented in Figure 4, and their relationships are briefly illustrated in Figure 5.

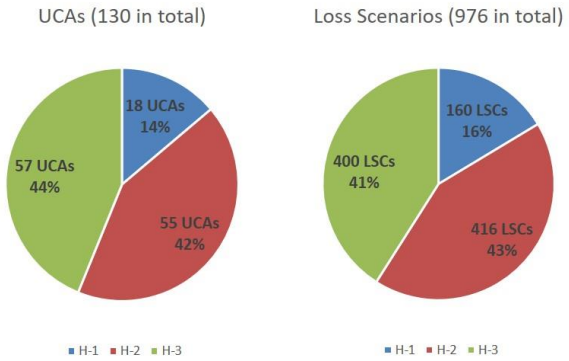

Figure 4 Number of UCAs and loss scenarios with related system-level hazards

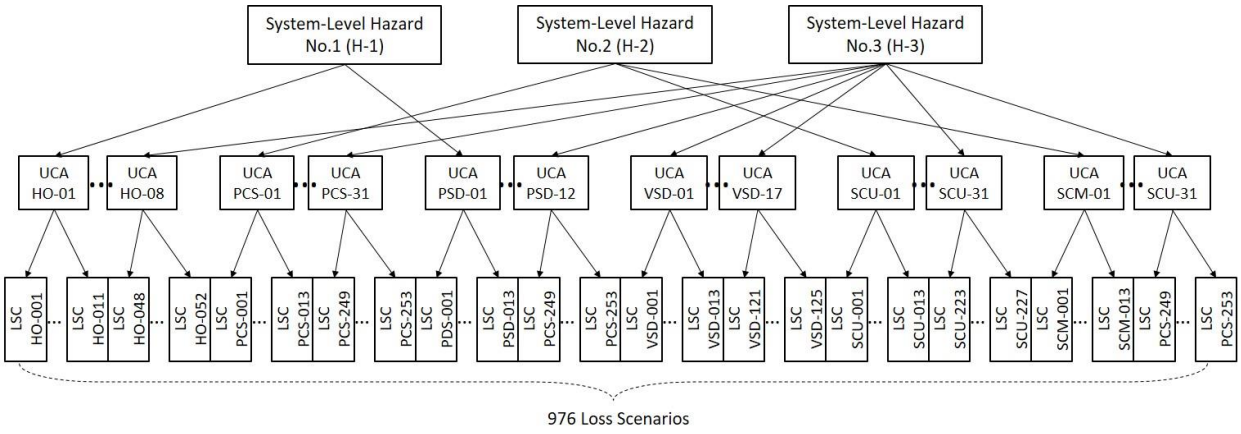

Figure 5 Relationships among system-level hazards, UCAs and loss scenarios

This case study was conducted with medium level of details, and the results of this analysis might be further refined. For instance, an example of a loss scenario is

> ***LSC.HO-022***
> *The processing condition is not optimal, but the Human Operator does not provide "Adjust set-point" command to the PCS [UCA.HO-04], because the Human Operator incorrectly believes that the processing condition is optimal. This flawed process model will occur if the sensors drift and provide wrong measurement. As a result, the gas compressor operates with reduced capacity [H-3].*

This scenario can further refined, because there are several sensors related with this scenario, such as compressor inlet pressure sensor, outlet pressure sensor, inlet temperature sensor, outlet temperature sensor, and so on. If the analysis is refined into a detail level, then tens of thousands of loss scenarios might be identified.

Managing tens of thousands of problems and developing/implementing solutions for each problem can be a challenging task. Furthermore, STPA does not evaluate the importance/criticality of the various results of the analysis, so all the problems identified by STPA must (in principle) be treated equally. However, this can be highly inefficient, because some problems are critical with severe consequence, while the others are not. Consider for example the following two UCAs from the case study:

> ***UCA.PCS-09***
> *PCS does not provide "Open ASV" command when compressor outlet pressure is higher than surge limit*
>
> ***UCA.PCS-21***
> *PCS does not provide "Speed Up Compressor" command when inlet flow is below optimal condition*

The consequence of UCA.PCS-09 is a serious damage of the compressor that causes enormous economic loss. In addition, when UCA.PCS-09 occurs, the compressor becomes damaged in less than a second, which means that correcting the UCA is almost impossible once it has occurred. On the other hand, UCA.PCS-21 causes minor economic loss, and there should be enough time available to correct it. Treating these two UCAs equally is not efficient if the aim is to improve safety within a given resource constraint. If we can evaluate the importance/criticality of UCAs, then we can prioritize the more critical and more important UCAs, so we can optimally spend our efforts to improve the safety of the system. The same applies to loss scenarios. The first challenge identified in this study is therefore

"UCAs and loss scenarios need to be evaluated and prioritized"

Once UCAs and loss scenarios are evaluated, we can also screen out minor problems from the analysis. Screening out minor problems can be particularly effective in STPA compared to other traditional methods, because STPA is a top-down approach. If we can screen out UCAs that have minor impact, then we can save a large amount of resource that would be spent to identify scenarios from the minor UCAs, as shown in Figure 6. This effect increases significantly when we refine the scenarios into detail. The more we develop details of the analysis, the higher the effect of screening becomes, because we can prevent the explosion in the number of loss scenarios early. The second challenge identified in this study is therefore

"Minor UCAs need to be screened out before identifying loss scenarios"

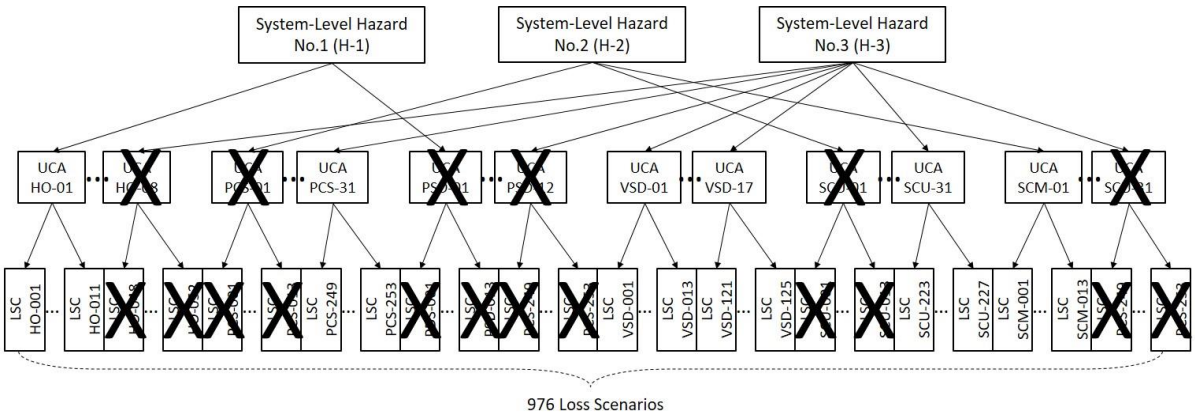

Figure 6 Screening out minor UCAs

4. A Solution to the Challenges

While STPA was developed to overcome limitations of traditional methods, this does not mean that we cannot learn anything from the traditional methods. Evaluation of hazardous events, including screening and prioritization, has been a cornerstone of many traditional methods. In this section, we therefore investigate traditional methods with focus on evaluation of hazardous events. After identifying limitations of the evaluation process of the traditional methods and providing solutions for the limitations, new procedures for STPA to evaluate UCAs and loss scenarios are proposed.

4.1 Learning from Traditional Methods

In this paper, we will not review methods in detail, and the reader may refer to two textbooks [19, 20], which give an overview of traditional hazard identification methods and provide useful references.

HAZard and OPerability (HAZOP) study was developed in the 1960s to identify hazards and operability problems for a process plant. In HAZOP, the system is divided into study nodes, and possible hazards are identified by brainstorming using pre-defined guidewords and process parameters. HAZOP formulates a list of hazardous events with associated consequences, existing barriers, and proposed improvements. The results of the HAZOP study are evaluated using Risk Priority Number (RPN), if needed. Likelihood (frequency) and consequence (severity) are normally used as criteria of RPN.

Preliminary Hazard Analysis (PHA) was derived from the U.S. Military Standard System Safety Program Requirements to reveal potential hazards, threats and hazardous events early in the system development process. The output of PHA is a list of hazards and generic hazardous situations including associated potential causes, effects, and preventive measures. The results of PHA are also evaluated using RPN, when necessary. Frequency and consequence are normally used as criteria of RPN.

Failure Modes and Effects Analysis (FMEA), one of the first systematic techniques for failure analysis, was developed in the late 1940s to identify hazardous events in military systems. FMEA reviews single failure modes and identifies their resulting effects on the rest of the system. The output of FMEA is a list of single failure modes that either directly result in or contribute significantly to an accident, including their causes, effects on the system, and risk-reducing measures. The results of FMEA can be evaluated using RPN, and this is called Failure Modes, Effects, and Criticality Analysis (FMECA). Frequency, consequence, and detectability are commonly used as criteria of FMECA.

All the three traditional methods introduced above adopts RPN to evaluate the results of the analysis. RPN is a number that represents risk level associated with each hazardous event, and is widely used in FMECA in particular. In FMECA, RPN contains three factors as below [21, 22]

- Severity (S): Result generated from failure
- Occurrence(O): Probability of a failure
- Detection(D): Opportunity for an unidentified failure because of the difficulty of defect detection

On the basis of degree, the three factors are scored from 1 to 10 (or 1 to 5, sometimes), and RPN is then obtained from the product of severity, occurrence, and detection, which can be expressed as below equation [21]

RPN = S x O x D

In addition to this basic approach, many studies introduced improved approaches to utilized RPN for FMEA. Some representative improvement were introduced by Xiao, Huang [23], Zammori and Gabbrielli [24], Chen [21], Sellappan and Palanikumar [25], Chen and Lee [26], Sellappan and Palanikumar [27], and Kharola and Singh [28].

RPN is a widely used and a proven approach that can be utilized for evaluation of STPA results, but there are still some limitations that need to be solved before we apply RPN approach to STPA.

4.2 Limitations of Traditional Methods and Solutions for the Limitations

1) Lack of knowledge can mislead us

As introduced in Section 1 and 3, several studies argued that assigning poorly founded probabilities/frequencies to hazardous situations may dangerously mislead us to omit important causal factors of an accident [1, 8, 9]. This problem with how quantitative risk assessment are often done was also discussed by Aven [29], Nilsen and Aven [30], and Aven and Renn [31]. To emphasize the importance of uncertainty (uncertainties of what will be the consequences) in risk assessment, Aven [32] proposed a new definition of risk as below

Risk is equal to the two-dimensional combination of events/consequences and associated uncertainties.

Or, in abbreviated form,

Risk = (C,U),

where C is the consequences of an activity, and U is the associated uncertainty. This view has also been adopted by the Society for Risk Analysis [33] and is similar to the most recent definition adopted by the International Organization for Standardization ("risk is the effect of uncertainty on objectives" [34]). The Petroleum Safety Authority (PSA) Norway [35] also provides a similar definition of risk;

Risk means the consequence of the activities, with associated uncertainty.

Flage and Aven [36] emphasized that uncertainties can be implicit in the background knowledge when the analysts make assumptions in a risk analysis, and altered background knowledge can decrease or increase the level of uncertainty. Accordingly, Aven [37] introduced the concept of *Strength of Knowledge* that is also called as *Level of Knowledge*. The *Strength of Knowledge* can be assessed using qualitative categorizations, and Flage and Aven [36] provided three categories of *Strength of Knowledge* that are listed in Table 2.

Table 2 Three categories of Strength of Knowledge [36]

Strength of Knowledge	Description
Low	One or more of the following conditions are met: • The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions. • The assumptions made represent strong simplifications. • Data are not available, or are unreliable. • There is lack of agreement/consensus among experts.
Medium	Conditions between those characterizing Low Level of Knowledge and High Level of Knowledge
High	All of the following conditions are met: • The phenomena involved are well understood; the models used are known to give predictions with the required accuracy. • The assumptions made are seen as very reasonable. • Much reliable data are available. • There is broad agreement among experts.

If we utilize this concept as an additional factor to evaluate UCAs and loss scenarios, the knowledge strength can be reflected in the evaluation of STPA results. We can therefore prevent dismissal of critical UCAs and loss scenarios for which the likelihood was judged to be low, but where the knowledge that this judgement was based on was poor, indicating high uncertainty.

2) Traditional criteria are not suitable for STPA

As introduced in Section 3, some UCAs leads to an accident instantly when the UCAs are provided, so we can hardly prevent occurrence of an accident or mitigate the consequence of the accident. Other UCAs, on the other hand, cause an accident only much later, so we can prevent an accident or mitigate the consequence even if the UCAs are provided. The criticality of an UCA can therefore vary in accordance with available time to response to the UCA, and therefore we need to include *Available Time to Respond* into the criteria to evaluate UCAs.

For the evaluation of UCAs, we can measure the consequence of an UCA, but likelihood can hardly be assessed. An UCA is a control action that will lead to a hazard in a particular context and worst-case environment [1]. It may be possible to estimate the likelihood of worst-case conditions to some degree, but we may not be able to assign accurate likelihood to a control action. Even though we can estimate the likelihood of a control action roughly, it is difficult to calculate the likelihood of the UCA, because the control action and the worst-case conditions might be dependent from each other. Therefore, UCAs can be evaluated by three criteria: *severity, available time to respond, and strength of knowledge on UCA*. Likelihood can be assigned to loss scenarios with associated strength of knowledge, and severity can be inherited from associated UCAs.

3) Traditional methods screen out minor problems at the end of the analysis

The traditional hazard identification methods utilize RPN to evaluate and screen out minor hazardous events, but this screening is conducted at the end of the analysis. Therefore, we cannot maximize the efficiency of the screening. If we can screen out minor problems from the early or middle stage of the analysis, lots of unnecessary further effort can be saved. This is impossible for traditional methods with bottom-up approach, but STPA can screen out minor problems from the early stage of the analysis, because STPA is a top-down approach. For instance, if we can screen minor UCAs at STPA step 3, a large number of loss scenarios do not need to be investigated at STPA stage 4, as shown in Figure 6.

4.3 Additional Procedure for Screening and Prioritization of STPA

The results from the previous sections have been used to suggest a new approach to evaluate, screen out and prioritize STPA results in this section. Four new sub-steps have been added to the original STPA procedure. After identifying UCAs (STPA Step 3), we evaluate UCAs, and screen out minor UCAs using RPN. The screened UCAs are then investigated to identify loss scenarios (STPA Step 4), and the identified scenarios are evaluated and prioritized in accordance with RPN of each scenario. The original STPA procedure and additional sub-steps for screening and prioritization are illustrated in Figure 7.

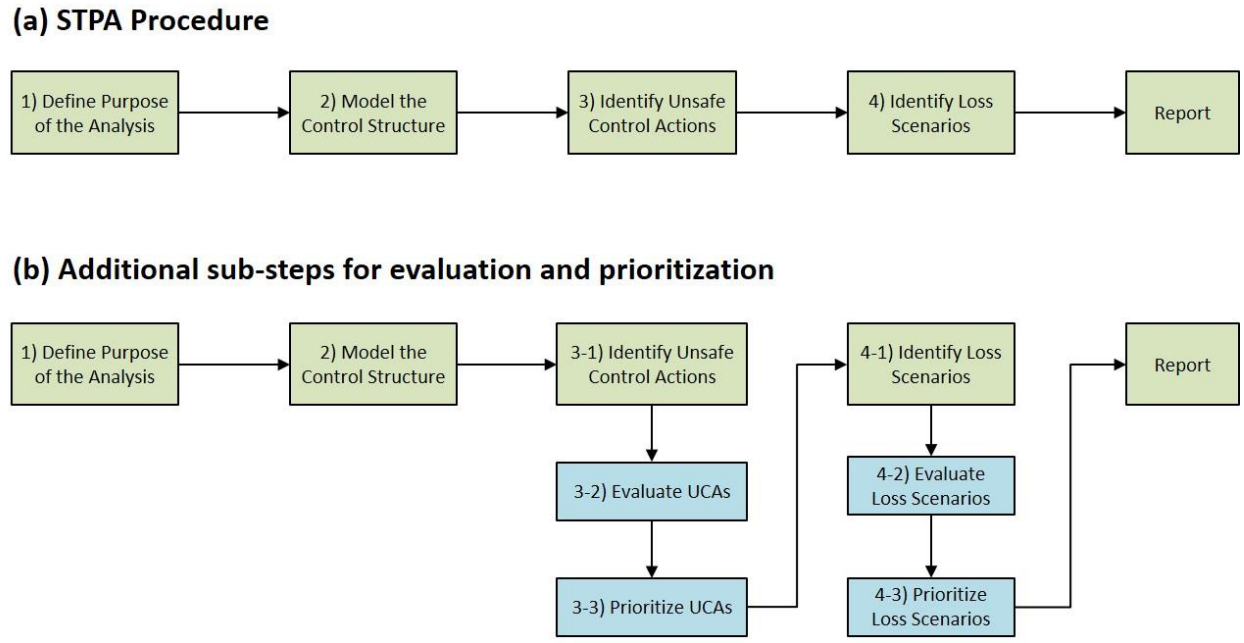

Figure 7 Original STPA procedure and additional sub-steps for screening and prioritization

To evaluate the results of STPA, we proposed five criteria: *severity, available time to respond, strength of knowledge on UCA, likelihood*, and *strength of knowledge on loss scenario*. Each criterion has five categories, where category five means the worst situation and category one means the best. For the evaluation of UCAs, three criteria can be used: *severity, available time to respond*, and *strength of knowledge* on UCA. Classification of *severity* was adopted from [20], and the other two criteria were originally proposed in this study. *Available time to respond* was established to evaluate how fast an UCA leads to an accident, and *strength of knowledge* for an UCA was developed based on the three knowledge levels proposed by Flage and Aven [36], which represents the analyst's overall knowledge level on the UCA. For the evaluation of loss scenarios, two criteria were introduced: *likelihood* and *strength of knowledge* on loss scenario. Classification of *likelihood* was adopted from [20], and *strength of knowledge* for a loss scenarios was developed to evaluate level of knowledge on the occurrence of the scenario. Criteria for the evaluation of UCAs and loss scenarios are listed in Table 3 and Table 4 respectively.

Table 3 Evaluation criteria for UCAs

Criteria	Category and Description
Severity* (SV)	5. Catastrophic loss to human, environment, and/or property 4. Severe loss to human, environment, and/or property 3. Major damage to human, environment, and/or property 2. Damage to human, environment, and/or property 1. Minor damage to human, environment, and/or property
Available Time to Respond (ATR)	5. Not possible to prevent occurrence of accident after UCA 4. Accident can be prevented or mitigated, only if required action is provided instantly 3. Accident can be prevented or mitigated, if required action is provided in time 2. UCA causes accident rather slowly, so we have some time to respond to UCA and prevent or mitigate accident

	1. UCA causes accident very slowly, so we have far enough time to respond to UCA and prevent or occurrence of accident
Strength of Knowledge on UCA (SOK)	5. Complex control action with no or little experience 4. Complex control action with a small number of experiences 3. Complex control action with a large number of experiences 2. Straightforward control action with a small number of experiences 1. Straightforward control action with a large number of experiences

* For details of classifications of severity, readers can refer to [20].

Table 4 Evaluation criteria for loss scenarios

Criteria	Category and Description
Likelihood* (LH)	5. Event that is expected to occur frequently 4. Event that happens now and then and will normally be experienced by the personnel 3. Rare event, but will possibly be experienced by the personnel 2. Very rare event that will not necessarily be experienced in any similar plant 1. Extremely rare event
Strength of Knowledge on loss scenario (SOK)	5. Complex scenario with no or few experience 4. Complex scenario with a small number of experiences 3. Complex scenario with a large number of experiences 2. Straightforward scenario with a small number of experiences 1. Straightforward scenario with a large number of experiences

* For details of classifications of likelihood, readers can refer to [20].

With above criteria, we can obtain RPN for an UCA and for a loss scenario from the following equations.

$RPN_{UCA} = SV \times ATR \times SOK_{UCA}$

$RPN_{Loss\ Scenario} = RPN_{UCA} \times LH \times SOK_{Loss\ Scenario} = SV \times ATR \times SOK_{UCA} \times LH \times SOK_{Loss\ Scenario}$

5. A Case Study

We demonstrated the additional screening and prioritization procedures using subsea gas compression system introduced in Section 3. The results of the assessment were checked by the author team, and the author team included persons that have detailed insight to the design and safety of the subsea compression system. The construction of the system control diagram was also carefully examined, to evaluate on a suitable level of abstraction on the system.

In accordance with the proposed additional procedure in Figure 7 (b) in Section 4.3, 130 UCAs were evaluated for screening out. It was identified that the highest RPN was assigned to 19 out of 130 UCAs, while 38 UCAs obtained the lowest RPN. The distribution of RPN of each UCA is shown in Figure 8.

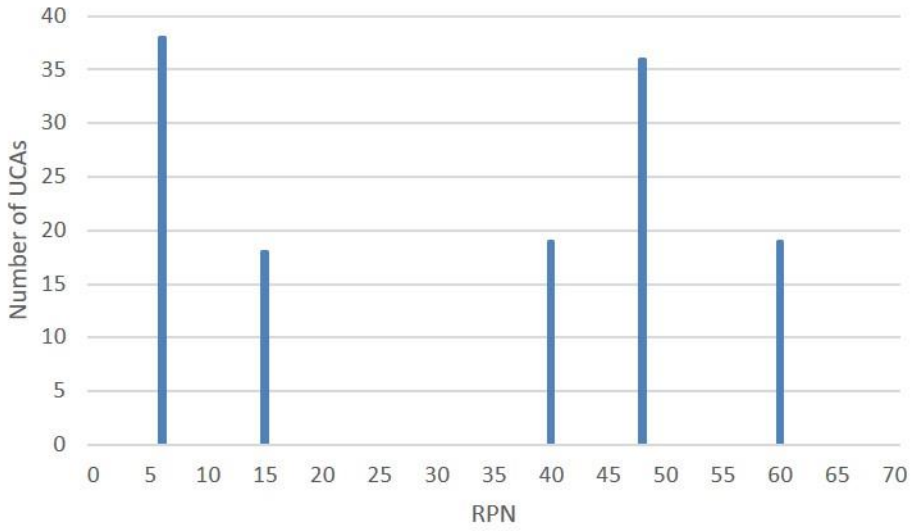

Figure 8 RPN Distribution of UCAs

In this case study, the 38 UCAs whose RPN are lower than 8 (about 10% of the highest RPN) were screened out. Some examples of highly ranked UCAs and screened out UCAs are provided in Table 5.

Table 5 Examples of highly ranked UCAs and screened out UCAs

	UCA	RPN
Highly ranked UCAs	**UCA.PCS-09** PCS does not provide "Open ASV" command when compressor outlet pressure is higher than surge limit [H-2]	60
	UCA.PCS-11 PCS provides "Open ASV" command too late when compressor outlet pressure is higher than surge limit [H-2]	60
	UCA.PCS-14 PCS provides "Close ASV" command when compressor outlet pressure is higher than surge limit [H-2]	60
	UCA.SCU-22 SCU provides "Close ASV" command when open ASV command is provided from PCS [H-2]	60
	UCA.SCU-23 SCU provides "Close ASV" command when no command is provided from PCS [H-2]	60
Screened out UCAs	**UCA.HO-04** Human Operator does not provide "Adjust Setpoint" command when processing condition is not optimal [H-3]	6
	UCA.HO-06 Human Operator provides "Adjust Setpoint" command too late when processing condition is not optimal [H-3]	6
	UCA.PCS-20 PCS provides "Speed Up Compressor" command when inlet flow is optimal condition [H-3]	6
	UCA.PCS-21 PCS does not provide "Speed Up Compressor" command when inlet flow is below optimal condition [H-3]	6
	UCA.PCS-23 PCS provides "Speed Up Compressor" command too short when inlet flow is below optimal condition [H-3]	6

While the consequence of H-1 is higher than that of H-2, UCAs connected H-1 got lower RPN, because we have a large number of experiences related to preventing H-1 and control actions available to manage H-1 are rather straightforward. All UCAs that had highest RPN were related to H-2 where strength of knowledge is much lower than the other hazards. In this respect, we could reflect

uncertainty of UCAs to the screening as we intended. Every screened out UCAs was related to H-3, but this does not necessarily mean that we can screen out H-3 in advance. Nineteen UCAs related to H-3 got higher RPN and were not screened out. If we had screened out H-3 in advance, we would have missed the 19 UCAs.

For the rest of 92 UCAs, 718 loss scenarios were identified, evaluated and prioritized in accordance with the procedure from 4-1 to 4-3 in Figure 7 (b) in Section 4.2. Forty nine out of 718 loss scenarios were assigned to the highest RPN, and 27 scenarios to the lowest RPN. The distribution of RPN of each loss scenario is shown in Figure 9.

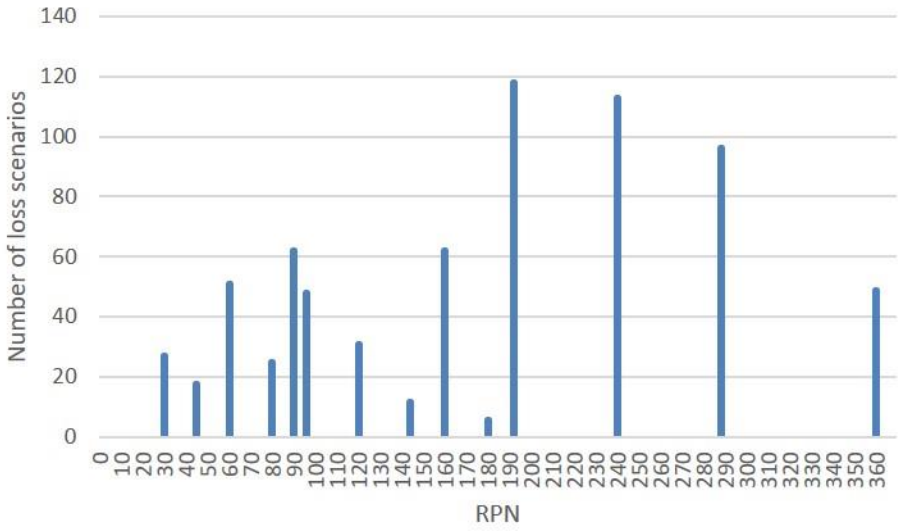

Figure 9 RPN Distribution of loss scenarios

Some examples of loss scenarios that have the highest RPN and lowest RPN and loss scenarios that were identified from screened out UCAs are presented in Table 6.

Table 6 Examples of loss scenarios with the highest RPN and the lowest RPN

	Loss Scenarios	RPN
Loss scenarios with the highest RPN	**LSC.PCS-071** PCS does not provide "Open ASV" command when compressor outlet pressure is higher than surge limit [UCA.PCS-09], because open valve command is not provided due to physical controller failure. As a result, a surge occurs at the compressor and the compressor is damaged [H-2]	360
	LSC.PCS-072 PCS does not provide "Open ASV" command when compressor outlet pressure is higher than surge limit [UCA.PCS-09], because open valve command is not provided due to electrical power supply failure to the controller. As a result, a surge occurs at the compressor and the compressor is damaged [H-2]	360
	LSC.PCS-112 PCS provides "Close ASV" command when compressor outlet pressure is higher than surge limit [UCA.PCS-14], because the PCS receives incorrect feedback due to drift of pressure sensors [PF]	360

Loss scenarios with the lowest RPN	**LSC.HO-007** Human Operator does not provide "Shutdown SGC unit" command when gas leaks to the environment [UCA.HO-001], because Human Operator receives no feedback due to communication cable failure. As a result, hydrocarbons leak to the environment, which leads to loss of human lives and environmental pollution [H-1]	30
	LSC.PCS-239 PCS does not provide "Shutdown Process" command to PSD when shutdown command is provided from Human Operator [UCA.PCS-29], because PCS receives no command from Human Operator due to signal cable failure. As a result, hydrocarbons leak to the environment, which leads to loss of human lives and environmental pollution [H-1]	30
	LSC.PSD-055 PSD does not provide "Close SDVs" command to SCU when shutdown command is provided from Human Operator and hydrocarbons leak to the environment [UCA.PSD-07], because PSD receives no feedback due to signal cable failure. As a result, hydrocarbons leak to the environment, which leads to loss of human lives and environmental pollution [H-1]	30
Loss scenarios identified from screened out by UCAs	**LSC.PCS-156** PCS provides "Speed Up Compressor" command to VSD when inlet flow is optimal condition [UCA.PCS-20], because PCS receives correct feedback, but control command is wrongly provided due to software flaw inside PCS. As a result, the compressor is operated under non-optimal condition [H-3]	24
	LSC.PCS-167 PCS does not provide "Speed Up Compressor" command to VSD when inlet flow is below optimal condition [UCA.PCS-21], because PCS receives correct feedback, but interprets incorrectly or ignores it due to software flaw inside PCS. As a result, the compressor is operated under non-optimal condition [H-3]	24
	LSC.PCS-169 PCS does not provide "Speed Up Compressor" command to VSD when inlet flow is below optimal condition [UCA.PCS-21], because PCS receives no feedback due to signal cable failure. As a result, the compressor is operated under non-optimal condition [H-3]	12

6. Discussions

6.1 Screening of UCAs

The original number of loss scenarios was 976 when we did not screen out UCAs, and after the screening, we could obtain 718 loss scenarios that is about 74% of the total loss scenarios (258 less critical loss scenarios were screened out). This means that if we apply screening of UCAs, then we can save our resource to identify 258 loss scenarios that is 26% of the total loss scenarios. The numbers of UCAs and loss scenarios before and after screening are presented in Table 7.

Table 7 Number of UCAs and loss scenarios with/without screening

	Without screening out UCAs (A)	With screening out UCAs (B)	Difference (B-A)
UCAs	130	92	38 (29%)
Loss scenarios	976	718	258 (26%)

At least for this case study, screening UCAs was efficient to reduce our time that we need to identify less important problems. However, we may be at risk to omit critical loss scenarios with the screening. An ideal RPN distribution is show in Figure 10 (a). RPNs of loss scenarios identified from critical UCAs should be higher than RPNs of loss scenarios identified from screened out UCAs. However, in this case study, some loss scenarios from critical UCAs had lower RPN value than loss scenarios from screened out UCAs as shown in Figure 10 (b).

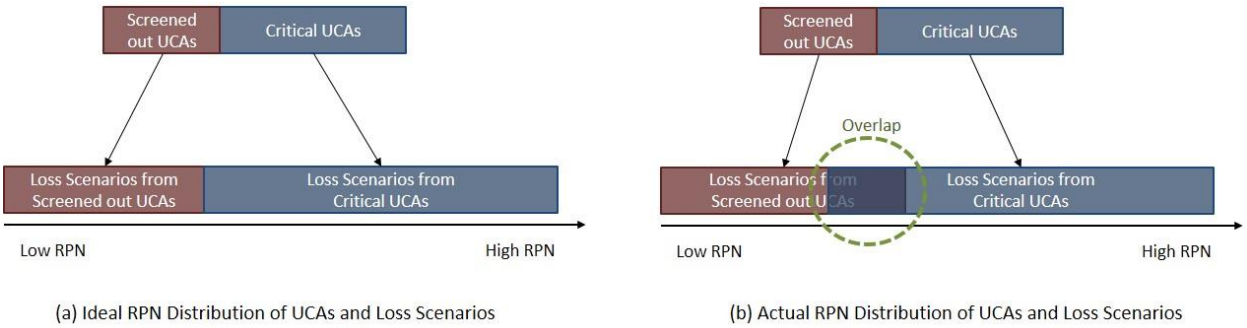

Figure 10 Ideal and actual RPN distribution

The lowest RPN of scenarios identified from critical UCAs was 30, so ideal situation is that the loss scenarios from screened out UCAs have RPN value lower than 30. However, in this case study, 92 loss scenarios had RPN higher than 30. The RPN distributions of loss scenarios from critical UCAs and screened out UCAs are shown in Figure 11. In this figure, we can find that some loss scenarios, which were not identified due to screening of UCAs, have higher RPN than the loss scenarios that were identified from critical UCAs.

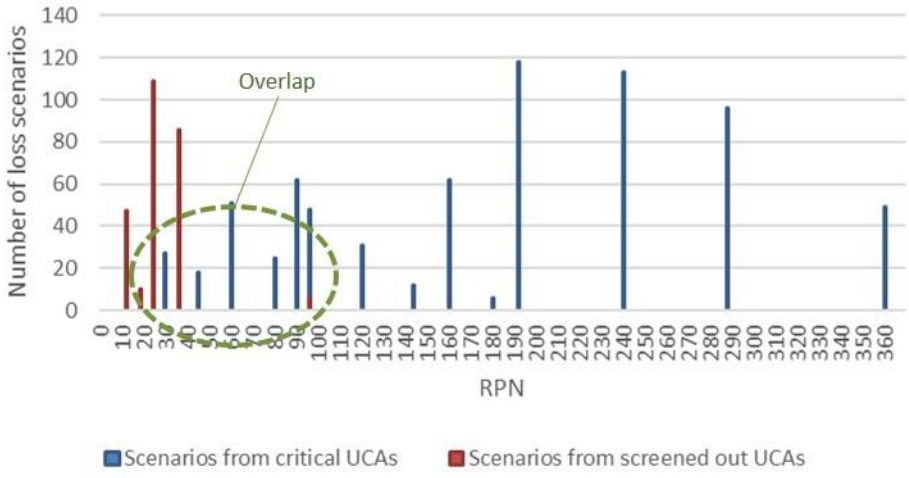

Figure 11 RPN distribution of scenarios from critical UCAs and screened out UCAs

This implies that relying on screening may mislead us to dismissal of important problems and focus on much less critical ones. The use of screening out UCAs must therefore be limited to specific circumstances when we lack time to investigate every UCA and loss scenario, and when we want to focus on serious problems only.

As illustrated in Figure 12, the original STPA ensures high safety but the efficiency might be low, because every UCA and loss scenario are treated equally, regardless of their criticality. STPA with screening and prioritization, proposed in this paper, allows flexible application of STPA. If we apply conservative screening, we can guarantee a certain level of safety with slightly improved efficiency. On the other hand, if we apply aggressive screening, we can improve the efficiency but cannot guarantee high level of safety. The analyst can make a decision between safety and efficiency depending on the circumstance. If we need a rough analysis with emphasizing highly important problems only, we can apply aggressive screening with spending less resource. For instance, in an early stage of a project, we may not have enough information to identify every detail and minor problems, and identifying all minor problems with limited information might be inappropriate. Then, we can apply STPA with aggressive screening. When we can obtain more information on the system, we can apply STPA with conservative screening. Finally, when we have every detailed information of the system, then we may apply the original (full) STPA without screening. This way of application can maximize our efforts to improve the safety of the system.

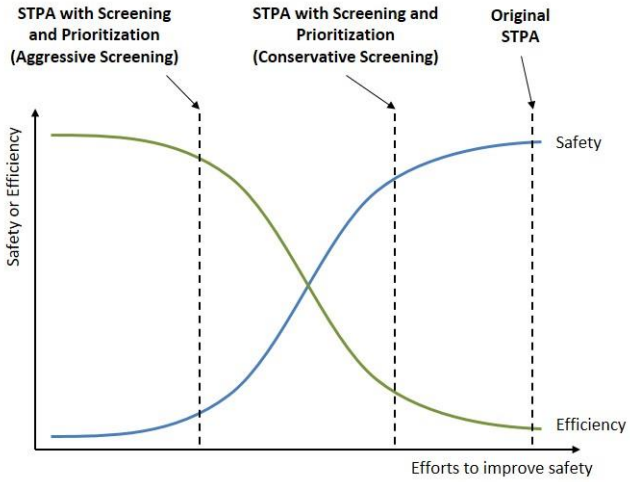

Figure 12 Safety and efficiency of each approach

6.2 Calculation of RPNs

In this study, RPN was obtained by the product of the score of each criterion, which is most widely used in traditional methods. However, there are other perspectives on the calculation of RPN. For instance, Rausand [20] proposed summing the score of each criterion to compute RPN, because there is no good theoretical justification for multiplying the scores and obtain RPN. Wheeler [38] argued that addition or multiplication of ordinal-scale data does not make any sense, because the lack of a distance function among the scores and the lack of an absolute zero may result in misjudgment on both serious and trivial problems. Rather, he proposed to generate a multiple digit code where each digit represents each

criterion. For instance, if a scenario has score 4 for severity, 3 for available time to respond, 2 for strength of knowledge on UCA, 3 for likelihood, and 1 for strength of knowledge on loss scenario, then we can generate a five-digit number as 43231, instead of multiplying the scores. We may change the order of each digit in accordance with the order of the importance of the criteria as shown in Figure 13. When these five-digit numbers are placed in descending numerical order, then they are prioritized by the order of important criteria. This approach can be used when the criteria have different importance and their hierarchy is clear. For instance, the five digits in above example, 43231, achieves a higher priority than 35555 in this approach, and this is reasonable only when the first criterion prevails all the other criteria. The appropriate approach to obtain RPN can vary depending on systems and operating conditions, so a further study is needed to find out the most suitable approach to obtain RPNs that can be utilized for STPA.

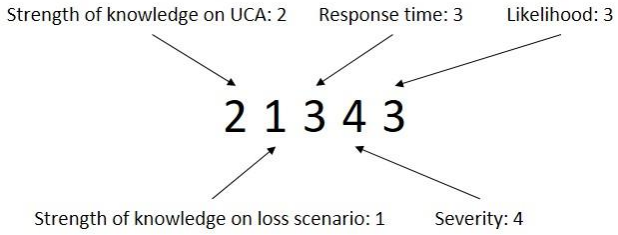

Figure 13 Generating a five-digit number with evaluation criteria

6.3 UCAs with multiple consequences

Some UCAs can cause multiple consequences. For instance, UCA.HO-01, *Human Operator does not provide "Shutdown SGC unit" command when hydrocarbons leak to the environment*, can lead to multiple consequences as below

1. A large number of fatalities and serious environmental pollution
2. A large number of fatalities with minor environmental pollution
3. A small number of fatalities with serious environmental pollution
4. A small number of fatalities with minor environmental pollution
5. No fatalities with serious environmental pollution
6. …

In this case study, we applied the worst-case scenario to evaluate UCAs, but this may not reflect reality when the variation of the multiple consequences is significant. A further study is needed to evaluate UCAs with multiple consequences, such as utilizing event tree analysis (ETA) to evaluate severity of an UCA.

6.4 Limitation - Evaluation criteria for other systems

We have used a subsea gas compression system to identify challenges in the prioritizing of results obtained with the STPA method, using the three new RPN criteria (including associated weight or score). At this stage, we cannot regard the RPN criteria as universal, meaning that they are applicable for all systems and industrial sectors, and further research is needed to evaluate their applicability for other case studies. At the same time, we believe that our proposal forms a good basis from the transparency provided for how the criteria have been derived. For instance, it is expected that the strength of knowledge will be applicable for most software-intensive systems, despite industry sector. Hazards may be omitted or their severity misjudged, if we have limited knowledge of and experience with a system. However, we foresee that different mode of operation or operating contexts can reveal the need for new or additional criteria. For instance, the subsea gas compression system is a highly automated system, so human intervention is limited in relation to operation as well as maintenance. Where the operation and maintenance of systems are dependent on human interaction, it is expected that also human-related evaluation criteria may be needed.

Consequently, at this stage we believe that more research is needed to derive classes of universal evaluation criteria that are found useful for different operating context and applications.

7. Concluding Remarks

In this study, we have proposed new procedural steps to the STPA method that allow prioritization of the analysis results. The challenge of STPA is that the method generates a large number of UCAs and loss scenarios without any evaluation, screening and prioritization, so highly critical problems and less important ones must be managed equally. To solve this issue, we investigated the application of RPN approaches with traditional hazard identification methods and proposed a set of RPN criteria that incorporate new elements. Finally, we proposed additional procedure steps to the STPA method for evaluation, screening and prioritization of STPA results using the new RPN criteria. The application of the new approach has been demonstrated using a subsea compression system as a case study. Still, we believe that more research is needed to evaluate how well the proposed RPN criteria will be valid when the operating context is changed. We encourage more research to investigate the possibility to converge towards a universal set of RPN criteria that can be applied with the STPA method.

Acknowledgements

This paper has been written under the Norwegian Centre for Research based Innovation on Subsea Production and Processing (SUBPRO, project 237893). The authors would greatly acknowledge to the financial support by the Research Council of Norway, as well to the industrial partners involved in this project.

References

1. Leveson N and Thomas J. *STPA Handbook*. 2018. Boston, MA, USA: MIT.
2. Leveson N. *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2012.
3. Fleming CH, Spencer M, Thomas J, et al. Safety assurance in NextGen and complex transportation systems. *Safety science* 2013; 55: 173-187.
4. Ishimatsu T, Leveson NG, Thomas J, et al. Modeling and hazard analysis using STPA. *4th IAASS Conference*. Huntsville, Alabama2010.
5. Abrecht BR. *Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System*. Massachusetts Institute of Technology, 2016.
6. Pawlicki T, Samost A, Brown DW, et al. Application of systems and control theory-based hazard analysis to radiation oncology. *Medical physics* 2016; 43: 1514-1530.
7. Sotomayor Martínez R. *System theoretic process analysis of electric power steering for automotive applications*. Massachusetts Institute of Technology, 2015.
8. Abrecht B, Arterburn D, Horney D, et al. A New Approach to Hazard Analysis for Rotorcraft. In: *Proceedings of the 2016 American Helicopter Society Technical Meeting, Huntsville, AL* 2016.
9. Leveson N and Thomas J. *An STPA primer*. 2013. Cambridge, MA.
10. Hafver A, Eldevik S, Jakopanec I, et al. Risk-based- versus control-based safety philosophy in the context of complex systems. *ESREL 2017*. Portorož, Slovenia2017.
11. Kim H, Lundteigen MA, Hafver A, et al. Application of Systems-Theoretic Process Analysis to a Subsea Gas Compression System. *European Safety and Reliability Conference (ESREL 2018)*. Trondheim, Norway2018.
12. Zikrullah NA. *Prioritization Approach for Systems-Theoretic Process Analysis (PA-STPA): Applied for Subsea Systems*. NTNU, 2018.
13. Thomas J. Systems Theoretic Process Analysis (STPA) Tutorial, http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf (2013, accessed 20 January 2018).
14. Fleming CH and Leveson NG. Improving hazard analysis and certification of integrated modular avionics. *Journal of Aerospace Information Systems* 2014; 11: 397-411.
15. Rising JM and Leveson NG. Systems-Theoretic Process Analysis of space launch vehicles. *Journal of Space Safety Engineering* 2018; 5: 153-183.
16. Leveson N, Couturier M, Thomas J, et al. Applying system engineering to pharmaceutical safety. *Journal of Healthcare Engineering* 2012; 3: 391-414.
17. Rokseth B, Utne IB and Vinnem JE. A systems approach to risk analysis of maritime operations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 2017; 231: 53-68. DOI: 10.1177/1748006x16682606.
18. Zhang J, Kim H, Liu Y, et al. Combining system-theoretic process analysis and availability assessment: A subsea case study. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 2019; 233: 520-536. DOI: 10.1177/1748006x18822224.
19. CCPS. *Guidelines for Hazard Evaluation Procedures*. Wiley, 2011.
20. Rausand M. *Risk assessment: theory, methods, and applications*. John Wiley & Sons, 2011.
21. Chen JK. Utility priority number evaluation for FMEA. *Journal of failure analysis and Prevention* 2007; 7: 321-328.

22. Automotive Industry Action Group. *Potential Failure Mode and Effects Analysis Manual, Ford Motor Company, General Motors Coropration*. 1995.
23. Xiao N, Huang H-Z, Li Y, et al. Multiple failure modes analysis and weighted risk priority number evaluation in FMEA. *Engineering Failure Analysis* 2011; 18: 1162-1170.
24. Zammori F and Gabbrielli R. ANP/RPN: A multi criteria evaluation of the risk priority number. *Quality and Reliability Engineering International* 2012; 28: 85-104.
25. Sellappan N and Palanikumar K. Modified prioritization methodology for risk priority number in failure mode and effects analysis. *International journal of applied science and technology* 2013; 3.
26. Chen J-K and Lee Y-C. Risk priority evaluated by ANP in failure mode and effects analysis. *Quality Tools and Techniques* 2007; 11: 1-6.
27. Sellappan N and Palanikumar K. Development of modified evaluation and prioritization of risk priority number in FMEA. *International Journal of Engineering (IJE)* 2013; 7: 32.
28. Kharola A and Singh S. Development of fuzzy failure mode effect analysis (FFMEA) model for risk priority number (RPN) analysis. *Advance Modelling and Optimization* 2014; 16: 211-222.
29. Aven T. On the need for restricting the probabilistic analysis in risk assessments to variability. *Risk analysis* 2010; 30: 354-360.
30. Nilsen T and Aven T. Models and model uncertainty in the context of risk analysis. *Reliability Engineering & System Safety* 2003; 79: 309-317.
31. Aven T and Renn O. On risk defined as an event where the outcome is uncertain. *Journal of risk research* 2009; 12: 1-11.
32. Aven T. A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability engineering & System safety* 2007; 92: 745-754.
33. Aven T, Ben-Haim Y, Andersen HB, et al. *SRA glossary*. 2015. The Society For Risk Analysis, Birmingham London.
34. ISO 31000:2009. Risk Management—Principles and Guidelines. Geneva: International Standards Organisation, 2009.
35. Petroleum Safety Authority Norway. Guidelines regarding the framework regulations, Section 11. Risk reduction principles. In: Norway P, (ed.). 2017.
36. Flage R and Aven T. Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability: Theory & Applications* 2009; 4.
37. Aven T. Practical implications of the new risk perspectives. *Reliability Engineering & System Safety* 2013; 115: 136-145.
38. Wheeler DJ. Problems with risk priority numbers. *Quality Digest Magazine* 2011.