Identifying safety indicators for safety performance measurement using system engineering approach

Sharmin Sultana[a], Bjørn Sørskot Andersen[b], Stein Haugen[a]

[a] *Department of Marine Technology, Norwegian University of Science & Technology, NTNU*
[b] *Department of Mechanical and Industrial Engineering, Norwegian University of Science & Technology, NTNU*

Abstract

This paper presents a method for development of safety indicators based on system engineering concepts. The use of system engineering in development of indicators may contribute to ensure that the process industry can operate their activities without any harmful accidents. Traditional approaches are either based on probabilistic risk assessment or occupational safety rather than system safety. These approaches assume accidents as linear chains of events; complex systematic factors and interactions are not considered. The report of the Baker review panel, after investigation of the BP Texas City refinery accident that occurred in 2005, suggested that BP had a false sense of safety performance due to giving more focus on managing personal safety rather than process safety. This paper adopts the approach of a system-based accident causation model, developed by Nancy Leveson, to identify system specific leading indicators. Additionally, it compares the developed method with other methods for practical case applications. The first step of the present method is to establish the safety control structure, then safety performance indicators are identified. Further work is necessary to investigate to what degree these STAMP (System-Theoretic Accident Model and Processes) based indicators are complementary to other safety performance indicators.

1 INTRODUCTION

An indicator is a measurable representation of the aspect of reality. Wreathall (2009) defines safety indicators as proxy measures for the items carrying importance in underlying models of safety. Safety indicators can be used to monitor the level of safety in a system to provide the necessary information for decision-makers about where and how to act (Hale, 2009). In the process industry, it is not easy to establish the relationship between accidents and process safety. Researchers (Guastello, 1993, Clarke, 2006, Tarrants, 1980, Lehtinen and Wahlström, 2002, Mearns et al., 2003) have tried to establish general relations between safety performance and contributing factors, i.e. the quality of safety management elements or the adequacy of the safety climate. However, accidents occur due to a confluence of multiple factors.

Accident investigations (Benner, 1975, CSB, 2007, Mogford, 2005) reveal that accidents could have been prevented if control actions were properly implemented as many of the problems were known prior to the accidents. One of the most challenging issues is to recognize the deterioration in safety performance as early as possible before any accident. Many accidents/incidents have taken place in process facilities in the past which were concluded to occur due to failure of equipment. This may be the direct cause but underlying this has often been lack of identification of deterioration of machines or failure to understand the condition of the asset. Inadequate attention to the safety performance resulted in cases like the Ciniza oil refinery explosion (CSB, 2005), the Mexico City refinery accident (Lees, 2012), the Balongan LPG Plant accident (Clough, 2009) and BP's Texas City refinery accident (Baker et al., 2007). Before the BP Texas City refinery accident, attention was only on the injury rate, but it was deficient in overall safety culture and in particular the process safety management program (Mogford, 2005). Several inspections were carried out by OSHA due to fatalities in the refinery. No

priority was given to enforce process safety regulations. According to the accident investigation (Baker et al., 2007), process safety elements such as mechanical integrity, training, leadership, and Management of Change (MOC) were deficient despite having excellent personal safety performance.

Nuclear power and chemical process industries use safety modelling techniques (e.g. probabilistic safety assessments) to identify likely contributors to accidents like failures of protective equipment and then trend the frequencies and durations for which such equipment is not operational. Some industries use techniques that involve some kinds of formal performance models and data-based evaluations of safety performance, e.g., the aviation and defence sectors. However, these are all very limited as sources of operational management information (Wreathall, 2006). Often, it is assumed that the frequency of small-scale accidents is an indicator for the probability of a larger one. This will be the case if the small accidents are part of the same population of accidents as the larger ones (Ale, 2009). If lost time injury rate (LTI) is considered as an indicator for process safety, the relationship between lost time injury rate and probability of accidents should be established first. They may not have the same causes and same accident mechanisms.

Another fact is that occurrence of a disaster by itself does not say anything about the quality of the installation, of the personnel or of the management (Ale, 2009). To develop process safety indicators, the process industry uses guidelines based on the concepts of the Swiss Cheese model or the Accident Pyramid. These guidelines view indicators as independent measures of the safety of a system, but they do not identify ineffective controls or interdependencies between barriers. Organizational aspects are covered, but not in a systematic way. They are often based on risk management programs that are either reactive (lack of forward-looking approach) or fragmented (system-based models are not used) (Khawaji, 2012).

Although a lot can be gained by using existing methods, there are challenges yet to be solved. For instance, methods for the development of proactive indicators, such as organizational indicators, still lack consensus. There is no unique approach concerning terminology and definition of ‘‘performance indicators,’’ ‘‘safety indicators,’’ and ‘‘safety performance indicators.” Evaluation of safety performance indicators is based on threshold values derived from experience. Historical data from accidents will, in practice, always be out-of-date as a measure of today’s performance. Over a period of many years, operations, training, technology, regulations and other aspects will change, implying that historical events may not necessarily be relevant anymore and that new hazards may have been introduced. The interpretation of these types of data is uncertain, often biased to find simple explanations and based on overly simple ‘models of safety’ that seek to identify one or two ‘root causes’ of accidents, neglecting the complexity of system (Wreathall, 2006).

Probabilistic safety assessments (PSA) and similar models are static interpretations of how accidents occur, focusing usually on descriptions of how combinations of hardware faults and operational errors may cause bad outcomes and neglect the complexity and interactions seen in complex accidents. Reviews of PSAs, when compared with major accidents, show that they typically fail to identify underlying organizational processes that override the usual assumptions of independence of failures, and neglect the complexities of human behaviours usually involved in accidents, often treating humans as if they were simple machines. (Wreathall, 2006). What are required are data that allow the organization’s management to know the current state of the safety performance within the organization, without suffering the problems outlined above.

Presently existing approaches emphasise technical limitations and ignore the role of cultural and organizational influences. They also emphasise lagging indicators, developed and based on past events, instead of focusing on leading indicators. A large missing piece is the lack of integration in the control of safety between technical entities and management/organizational entities. A safety management system can be fully effective only when it considers the full system, along with its complex interaction within its subsystems, dynamics, and if interaction with its subsystems is proactive enough to enable early action (Rasmussen 1997). This paper adopts a system-based model to address system aspects that enable detection of ineffective control and degradation of the system. It adopts STAMP based modelling (Leveson, 2004) to develop leading indicators. STAMP provides a better understanding of

the system, helps in identifying better means for developing safety indicators, assists in monitoring a system's status and thereby helps to make quicker decisions to prevent accidents from occurring.

The present paper is structured according to a combination of two main tasks. The first task is related to the development of system-based safety indicators. The second task is to make a comparison between the present developed method and another established method already used by industry. The first task starts by searching for the causes of accidents of a system and further searching for causal factors, including technical, human, and organisational causes by establishing a relationship between a system and its controllers.

The paper develops system-based process safety indicators for an LNG floating storage platform. Technical and organizational safety indicators are developed to ensure effective control structure. This can help plant managers and decision makers in proactive risk management by monitoring contributing factors in systematic ways in order to prevent accidents before they occur. The proposed method is compared with the OECD guidance (2003) on safety performance indicators. The article is structured as follows: the following section gives an overview of previous work on methods for development of performance indicators. The methodology developed in the present analysis is described in the "Methodology" Section. The "Application" section presents the case study before the analysis is discussed in the "Discussion" section. The final section, "Conclusion," states the conclusions.

2 PREVIOUS RESEARCH ON DEVELOPMENT OF INDICATORS

Work on the development of performance indicators has been driven by two different directions: leading indicators and lagging indicators. There has been a lot of dispute among safety professionals and researchers about the definition and use of lagging and leading indicators. The first dispute is on the definition of the terms. Hopkins (2009) defined leading indicators as ''precursors of harm" as opposed to lagging indicators that are ''direct measures of this harm".

The Swiss cheese model describes accidents as a series of failings (holes) in the layers of defences or barriers. According to this model, leading indicators identify holes in the risk control system, whereas the lagging indicators reveal the holes in the barriers as a result of an incident. Hollnagel (2017) has discussed these issues from the system engineering perspective. According to his theory, leading indicators can be created based on the sense of perturbations in the parts of the system where fluctuations may be observed to see how stable the system is. In contrast, lagging indicators generally provide evidence of an effective safety system by observing whether any anticipated consequences of changes have been observed.

An accident is characterised by the loss of control of energies. Process accidents involve loss of containment of hazardous media in a process plant. In major accidents, a large amount of energy is released causing multiple fatalities, and/or substantial environmental and material damage. It will not be possible to develop leading safety performance measures unless the relationships between losses, types of energy involved, and precursors are well enough understood (Kjellén, 2009).

According to Erikson (2009), lagging performance indicators are focusing on the output and are indeed providing the best measure of how well the management system is performing. The leading performance indicators are focusing on the input and tells us how to achieve the main objective and how to improve it. In this sense, there is a fundamental difference between leading and lagging indicators, and both are needed to determine how well process safety is managed in the organization. A specific indicator could be lagging in relation to one objective, while leading in relation to another. "Failure at testing" is lagging in relation to the performance of the individual barriers, while leading in relation to the performance of the overall process safety management system.

According to Hopkins (2009), lagging indicators are not very useful as pre-warnings or early warnings. For early warnings, one needs to look further back in the causal chain at the underlying causes and the condition of the factors that lead to accidents. These causes or conditions are termed as proactive, or indirect leading indicators. Hopkins argues that in the area of process safety, this distinction has no clear

meaning and that it is of relatively little value. He bases his argument on the fact that the bowtie model does not provide a good basis for the distinction between lead and lag. According to Vinnem et al. (2006), leading indicators are clearly preferred over lagging indicators. There is more motivation in reporting performance of preventive measures, compared to performance in occurrence of near-misses. If the data collection scheme is limited, the number of faults recorded will be insufficient to make a reliable decision. In that case, leading indicators are to be preferred over lagging indicators.

(HSE, 2006) emphasize the importance of utilizing both leading and lagging indicators and use the term 'dual assurance'. According to Grote (2009) and Kjellén (2009), the starting point could be to establish the purpose of indicators, describing the functions that they may have. Several authors do not distinguish between leading and lagging anymore. Because of this ambiguity a more general terminology is used, like key indicator, safety performance indicator, or key performance indicators (Saqib and Siddiqi, 2008, Grote, 2009, Mearns, 2009, Øien et al., 2011).

Often in literature, a distinction is made between risk indicator and safety indicator. In risk-based indicator models all risk influencing factors (RIFs) are included in a risk model, so it is possible to determine the effect on risk for a change in the indicator value of a given RIF. When it is termed as safety indicators, we do not have such a risk model. The indicators and the corresponding factors are then often selected, based on either an assumed effect on safety, or through correlation (Øien et al 2011). In this paper, the literature review is based on the nuclear industry and the process industry.

2.1 DEVELOPMENT OF INDICATORS IN NUCLEAR INDUSTRY

The nuclear power industry has been a key driver in the development of major hazard indicators. Two important directions were physical equipment performance safety and operational performance safety.

World Association of Nuclear Operators (WANO) was formed after the Chernobyl accident in 1986. Worldwide standardization of performance indicators was seen by WANO as one of the important aims. In 1990, WANO established a set of 10 performance indicators in the areas of nuclear power plant safety, reliability, efficiency, and personnel safety (Holmberg et al., 1994). Still, concerns have been raised regarding the extent of safety emphasis in the WANO indicator set. A practical problem for the operators is to sort out the most important information from the large flow that comes in every day. Improved learning from experience can be achieved by using more power plant specific safety indicators. Thus, further development and implementation of more detailed and plant specific indicators (for surveying safety critical activities and uncovering deviations in the power plant) were considered useful among nuclear plant operators as well as regulators (IAEA, 1991).

The WANO indicators may be classified as direct indicators; that is, outcome indicators that utilize different types of experience data. Whereas work has continued in developing direct indicators, emphasis has also been put into the development of indicators that can give early warnings. These early warning types of indicators are classified as indirect indicators, which can measure the performance of the functional units within an organization, such as operation, maintenance, training, and engineering support (Holmberg et al., 1994)..

In the Nordic project (described by Laakso et al. (1994)), the barriers in the defence-in-depth strategy along with the risk analysis were identified as a reasonable framework for identification and structuring of the safety performance areas. Barriers are physical or nonphysical systems which prevents energy from getting out of control, thereby reducing risk to assets and human beings. They should uphold the integrity for a defined time and energy limit. The performance areas defined, based on the defence-in-depth strategy, were: Safety management (Level 1 safety barrier), Control of operation (Level 2 safety barrier), Safety functions (Level 3 safety barrier), Physical barriers (Physical barriers 1–4). Indicators can be used to evaluate safety by assessing the performance level, and by evaluating the performance trend. Vattenfall developed operator specific safety indicators in continuation of the Nordic project. Holmberg et al. (1998) developed and tested risk-based PSA indicators. The indicators were used for

risk follow-up of events and unavailability of safety related systems. The main aim was to classify the safety significance of events, and not to use the indicators as a tool for "continuous" risk control.

The development of the IAEA framework (2000) for indicators began with the consideration of the concept of nuclear power plant safety performance. The framework was structured on two levels. The top level was operational safety performance and the 2nd level was operational safety attributes from which a set of operational safety performance indicators could be developed. To define the key attributes, three important aspects were addressed – nuclear power plant normal operation, emergency operation and the attitude towards personal safety. Below each attribute, overall indicators were established. Associated with each overall indicator was a level of strategic indicators, intended to provide a bridge from overall to specific indicators. Finally, each strategic indicator was supported by a set of specific indicators, which represent quantifiable measures of performance (Gómez-Cobo, 2002). In this framework, only the specific indicators are measurable quantities and higher-level indicators cannot be measured in terms of physical quantities. Higher-level indicators basically provide qualitative assessment.

2.2 DEVELOPMENT OF INDICATORS IN THE PROCESS INDUSTRY

In the process industry, development of indicators were driven by various accident models. Accident models try to explain why accidents happen and affect the development and use of risk assessment methods. They focus on different aspects and may reveal different causes of accidents. Accident investigations may provide useful input to development of safety indicators. In the nuclear and non-nuclear process industry, development of indicators can be viewed mainly with three main accident perspectives, which are Energy barrier perspecive, Resilience engineering perspective and System dynamic model.

2.2.1 Energy barrier perspective

Gibson (1961) introduced the Energy Model, saying that the easier way to classify the accidents is according to the physical energy form involved. Haddon (1970) did further work for accident prevention. The basic idea is that accidents occur when targets are affected by harmful energy in absence of effective barriers between the energy source and the object. Reason's (1997) Swiss cheese model is also based on the energy barrier perspective. Accidents occur due to holes in the barriers and safeguards. In an ideal world, all defensive layers should be intact allowing no penetration to happen. However, in the real world defences may deteriorate over time (such as the corroded sprinklers on Piper Alpha). Modification or redesign may weaken or eliminate defences. Defences can be removed during calibration, maintenance and testing or as a result of errors and violations.

In 1994, the NPD initiated a pilot project (Nielsen et al., 1996, Øien et al., 1997, Øien et al., 1998) with the purpose to develop a set of indicators that could be used to measure changes in risk level during the operation of petroleum platforms. Quantitative risk analysis (QRA) was used to identify risk indicators giving the most significant contribution to the total risk. The pilot project was followed by another project where a set of risk indicators was developed for a specific installation (Øien and Sklet, 1999).

Øien's (2001b) developed a risk-based method with the intention to cover the total risk picture. The model was based on the hypothesis that risk control can be achieved through control of changes in the risk influencing factors (RIFs) and most of the essential technical RIFs are included in the risk model in the QRA. The model did not cover "non-technical" risk indicators (human and organisational factors), but Øien (2001a) developed organizational risk indicators based on an organisational risk influence model (ORIM) resembling previous organizational factor frameworks (Davoudian et al., 1994a, Davoudian et al., 1994b, Embrey, 1992, Murphy and Paté-Cornell, 1996, Papazoglou and Aneziris, 1999).

Haugom and Friis-Hansen (2011) used a Bayesian network to model risk in a hydrogen refuelling station. Gerbec and Kontić (2017) also used a Bayesian belief network to establish process safety related key performance indicators. Their case study deals with ship tanker unloading of methanol at a liquid cargo terminal. Zhao et al. (2015) also used the Bayesian network modelling to analyse risk on LNG carrier anchoring system.

OECD started in 2003 to give guidance to the process industry at large through the Chemical Accidents Programme. The OECD guidelines methodology (2003) start by identifying critical potential hazards in various areas of concern that are most critical to control risk. Indicators are developed based on potential failures in the areas of concerns, or where there are ineffective barriers. The main new contributions of this guideline were differentiating outcome indicators (lagging) from activities indicators (leading) along with additional details on their development.

The development of the barrier-based indicators in the risk level project (RNNP) has been discussed thoroughly by Vinnem et al. (2006). The approach is based on recording occurrence of near misses and relevant incidents, performance of barriers and results from risk assessments. Indicators have been developed for each risk associated with major hazards on the installations and for performance of barriers that are installed to protect against these hazards. Khan et al. (2010) presented a risk-based approach where they used a risk metric to classify process safety. A hierarchical risk aggregation approach was used to aggregate indictors. Safety performance indicators (SPI) are developed considering UK HSE guidelines (2006) on the development of process safety indicators. The risk factor for three integrity categories: operation, mechanical, and personnel are aggregated using the weighted average approach. Three elements were monitored through a set of parameters and sub parameters characterized in two groups: leading and lagging indicators.

Haugen et al. (2012) developed a method to identify indicators not only related to operations and technical systems directly, but also to planning processes and other preconditions. The method uses a risk model to identify factors that influence the probability of a specific event. Risk influence modelling has been applied. For each factor, indicators that can measure the status of the factors are identified.

Sharp et al. (2008) developed key performance indicators for offshore structure integrity based on barrier analysis. Performance indicators were developed to monitor those barriers with quantifiable measures. Øien (2008) explores the possibility of developing early warning indicators based on incident investigation. The incidents are analysed using influence diagrams, from which seven general barriers against hydrocarbon leaks have been identified. For each barrier, both checkpoints and indicators have been developed, which provide information about the status of barriers and the early warning of potential spills.

The UK HSE guidance (2006) describes a method based on the Swiss Cheese model. A key addition of this guidance was the introduction of the “dual assurance” concept requiring both leading and lagging indicators. Leading indicators are developed based on barrier failures that are discovered during reviews, while lagging indicators are developed based on failures that are discovered after an incident or near-miss has occurred.

Thieme and Utne (2017) used both dual assurance method and resilience based early warning indicators (REWI) method to develop safety indicators of autonomous marine system. They showed in their paper that these two methods are complementary and how two methods can be integrated and applied jointly. If applied separately would overlook important safety aspects. If combined, gives complete coverage of safety aspects. Developing SI is most efficient if implemented during design stage and can be refined based on operational experience. Implementation during operational phase is challenging concerning collection due to necessary interfaces. For AUV, developed five outcome and 11 early warning indicators. Developed indicators cover direct safety function e.g. alarm and broader safety function e.g. maintenance. Relationship between safety and Sis is inferred.

System dynamic model

In systemic models the whole system is looked at as one entity, not as being made up by several components. System based indicators are based on identified system risks.

2.2.2 Resilience engineering perspective

Resilience Engineering is not about assessing accident risks, but assessing the organization's ability to be resilient (succeed) in the face of expected and unexpected vents. Øien et al. (2010) describes a method for the development of early warning indicators based on resilience and resilience engineering (REWI). The method is based on a method developed by the U.S. Electric Power Research Institute (EPRI) known as Leading Indicators of Organizational Health (LIOH) (EPRI, 2000, EPRI, 2001). REWI consists of three main parts. The first part is a set of contributing success factors being attributes of resilience, the second part is general issues to ensure that the goal of each contributing success factors is fulfilled, and the third part is the indicators established for each general issue. Indicators established by other approaches can be included in the final selection of indicators.

According to Paltrinieri et al. (2012), the dual assurance method (HSE, 2006) strictly depends on the results from the HAZID process. A lack or flaw in the HAZID process would affect all the subsequent analyses, and an unrecognized scenario would not be properly tackled by indicators. On the other hand, REWI is not dependent on the specific HAZID outcome. It is complementary to the result of HAZID and supports risk appraisal through a parallel and comprehensive action of organizational improvement.

A contribution from the resilience theory is Reiman and Pietikäinen (2011), which classify safety performance indicators into three groups, depending on their purpose. These are lag indicators, measuring the outcome of an activity, and two kinds of lead indicators: indicators for driving and for monitoring. The authors also proposed a wide range of indicators within three categories. These indicators have also served as inspiration for the selection of indicators in this paper, but many of these are general in character and difficult to measure on a regular basis.

2.2.3 STAMP

The STAMP accident model, proposed by Leveson (2004), is based on system theory, which is based on non-linear events and dynamics as well as feedback or feed-forward control. The method adopted in the present paper is based on STAMP model. Detail procedure of the method is described in the following section.

3 METHODOLOGY

In STAMP, safety is an emergent system property and safety should be treated as a control problem for complex systems. Risk management efforts should not only focus on addressing previous accidents, because different interactions of the system and social aspects may result in unforeseen inadequate control. STAMP includes a new hazard analysis method called STPA (System Theoretic Process Analysis), which is built on STAMP as a theoretical foundation. STPA can be used to identify safety constraints that can form the basis for a leading indicator program.

In STAMP, accidents are caused by unwanted interactions among system components that violate system safety constraints. An example of safety constraints is that a highly reactive chemical must be stored below a maximum temperature. The constraint must be enforced in the operating process and contingency action must be taken if the constraints are somehow violated. STAMP views process or system safety as a control problem. Accidents occur when system components (physical and social) are not adequately controlled. The controls may be managerial, organizational, physical, operational, or manufacturing. Major accidents occur due to not only component failure or human error, but also from inadequate enforcement of safety constraints on design, construction or operation of the entire socio-technical system (Leveson, 2015).

To monitor the performance of the system, analysis should ensure the identification of factors resulting in potential flaws, both at system level and component level. Development of safety performance indicators can be performed by following the below steps:

1. Description of system boundaries and the control structure of the system
2. Identification of system level hazards, accidents and safety constraint
3. Identification of required control actions to keep the system safe
4. Identification of the low-level contribution factors or scenarios that results in hazardous situations
5. Determination of corrective actions to rectify the hazardous causes
6. Identification of safety performance indicators
7. Development of performance monitoring program

3.1 Description of System Boundaries and Control Structure

The first step in STPA is to conceptualize the system as a control system and define the boundary of system. The control structure should be created using the system requirements and hazards. Each controller is assigned responsibilities involving avoidance of hazards.

The safety control structure of STPA provides an in-depth means for identifying potentially hazardous control actions by identifying system behaviors and interactions. This model of system behaviors defines feedback mechanisms between different responsible entities in the system. It identifies the paths for inadequate control of the system that can lead to a hazardous state.The system can consist of various controllers, actuator systems and disturbance processes (e.g. wind, waves, current). The control hierarchy diagram provides the means to visualize the interactions between controller, actuator and actual process.

The controllers provide control actions to keep the system under controlled situation. Feedback may be physical, e.g. physical sensors which provide information to low level or high-level controllers about the state of the system at that point of time. Controllers give commands to an actuator to take necessary action. A controller can be an automated logic controller or human (e.g. control room operator). An actuator can be physical e.g. pressure relief valve which gets opened when the controller gives a command to reduce pressure, getting feedback from the pressure sensor that pressure is too high in the system. A human actuator may work also, e.g. the local operator may reduce the pressure manually. Control can be provided not only by engineered systems and direct management intervention, but also indirectly by policies, procedures and other aspects of the organizational culture. The actuation system is composed of pumps, non-safety valves, thermal relief valves, emergency relief couplings, and emergency shut down valves.

3.2 Identification of System Level Hazards, Accidents and Safety Constraints

The first step of STPA is to identify the unsafe control actions that can lead to hazards.

In STPA, a hazard is a system state or set of conditions that, together with a set of worst-case operational and/or environmental conditions, will lead to an accident (loss event). An intermediate accidental event is an event in a sequence of events that upsets normal operations of the system and may lead to an unwanted accidental event or accident. If it is not controlled, it will lead to an accident. An intermediate accidental event is ‘leak in the system’, which if not controlled may lead to fire if ignited or explosion. Hazard are high temperature or pressure or other undesired situations in the system from which a leak may occur.

Safety constraints are those criteria that must be enforced on the behavior of the system to ensure safety. If hazards are not controlled, they may lead to accidents. The controller can be an operator or logic controller which can control the hazard preventing an accidental event or accident from occurring. For example, high pressure or high temperature can be reduced by operator or logic controller by opening

a thermal relief valve. Here, the safety constraint is the condition that a process should not exceed a predefined limit of temperature or pressure to keep the system safe.

3.3 IDENTIFICATION OF REQUIRED CONTROL ACTION TO KEEP THE SYSTEM SAFE

Accidents in complex system evolve from unsafe or inadequate control actions by automatic or human controllers. Unsafe control actions can be provided due to incorrect or missing feedback or due to miscommunication between multiple controllers.

There can be four types of hazardous unsafe control:

1. An action required for safety is not provided, e.g., the operator does not close the intake valve when the storage tank is full.
2. An unsafe control action is provided, e.g., the operator opens the intake valve when the storage tank is full.
3. A potentially safe control action is provided too early or too late, e.g., thermal relief valve is opened too late after detection of high temperature.
4. A control action required for safety is stopped too soon or applied too long, e.g., thermal relief valve is closed too soon before temperature is reduced to a safe level.

3.4 IDENTIFICATION OF LOW-LEVEL CONTRIBUTION FACTORS OR SCENARIOS

After the potentially unsafe control actions are identified, the next step in STPA determines how these unsafe control actions could occur or how the hazardous scenarios can evolve that can lead to a hazardous system state or accident. This step identifies the scenarios, where safe control is provided but the control actions are not executed correctly, perhaps because of a component failure in the controlled process. Determination of corrective actions to rectify the hazardous causes

The goal of the analysis is to identify hazards and then either to eliminate or to prevent them. If they cannot be prevented, then they need to be mitigated. This goal can be achieved by identifying the constraints underlying the hazardous scenarios identified by hazard analysis. The process for identifying required goals also gets important input from system hazard analysis and accidents.

The design of the safety control structure should enforce this constraint by allocating appropriate responsibilities for enforcing this requirement (safety constraint) and the feedback loops necessary to enforce it successfully. As an example, the chief engineer is responsible for technical standards and system safety requirements and for all changes, variances, and waivers to the requirements. The control actions on behalf of the chief engineer are:

- To develop, monitor, and maintain technical standards and policy
- To establish the technical requirements and to ensure that they are enforced and implemented in the projects
- To ensure the design is compliant with the requirements

Conditions meeting the above-mentioned requirements can provide important information if included in the leading indicator program. When the chief engineer cannot perform all the duties alone, he has the responsibility to ensure that the job is done by other responsible persons in the plant. To check the required control actions, responsibilities of all responsible entities should be carefully considered. Coordination risks arise when multiple people or groups control the same process. The types of unsafe interactions that may result include: (1) both controllers assume that the other is performing the control responsibilities and, as a result, nobody does or (2) controllers provide conflicting control actions that have unintended side effects. When similar responsibilities related to the same system requirements are assigned to multiple controllers, then the constraints that the control structure designers made about how the actions would be coordinated need to be recorded and used in the leading indicator program.

Important constraint may arise from safety culture. Cultural values and assumptions affect the establishment of the safety management system. Hard and fast rules may not work in all environments or may work in special cases, or may affect working environment, increase fatigue of a worker, and thereby may increase human error. These issues should be considered when determining safety constraints.

3.5 IDENTIFICATION OF THE SAFETY PERFORMANCE INDICATORS

In previous steps, hazards are translated into safety constraints. In the present step, possible safety indicators are identified from safety constraints. One or several indicators can be developed for each constraint. During the development of indicators, focus should be given on the properties of the system (e.g. dangerous substances, failures in the organizational structure). Focus should also be on hazards in the task that are carried out, like mechanical or electrical work.

Indicators should be developed based on the following topics of interest:

- Operability: How the organization will be able to keep the equipment or system in a safe and reliable functioning condition, according to pre-defined operational requirements.
- Design and engineering: Methodical constraints which should be included in designing functional products and processes.
- Training and competence: Training and competence necessary to develop among organization to operate the system smoothly
- Human resource management: Strategic approach to effective management of workers of organization so that they contribute to achieve overall goal in terms of safety. It is important that indicators detect problems at the facility level, not only on this system, so additional indicators are needed. For example, requirements for audit and procurement are important safety factors for process industry.

3.6 DEVELOPMENT OF PERFORMANCE MONITORING PROGRAM

Primary identification of indicators may result in a long list. Continuous monitoring of a large number of indicators is time and cost consuming. The final step therefore includes screening of indicators, setting the unit and target values for indicators and identifying the responsible entity.

The indicators must be updated at regular intervals, but the frequency of update depends on the type of operation and the indicator. For some systems, barriers need to be checked as frequently as every day. Indicators related to these barriers should be updated weekly or bi-weekly to identify any negative development. On the other hand, some indicators can be checked far less frequent, e.g. periodic maintenance of check valves.

4 CASE STUDY

4.1 DESCRIPTION OF SYSTEM BOUNDARIES AND CONTROL STRUCTURE

Main component of LNG ship to ship transfer process is pump. Other components include control valves, hoses, pipelines. Valves are used to control the nature of flow e.g. pressure, temperature, flowrate. Emergency relief valves or couplings can stop the operation or discoonetion the pipes to abort the operation in case of emergency.

A simplified process flow diagram is shown in Figure 1. Top filling of the receiving tank is commonly used to reduce the pressure in the tank. To start the transfer from tank 1 to tank 2, valves V3, V4, V7, V8, V11, V12 and V15 should be opened.

Figure 2 shows the high-level safety control structure of the STS transfer operation, where several agencies (LNG carrier authority, floating storage and regasification plant authority, and terminal authority) are involved in safety oversight of the operation. Each component in the control structure can control the behaviour of some lower level components in the structure. The present system has three types of controllers which are logic controller, control room operator and site operator. Controllers conduct the operation maintaining safe operational limit by providing appropriate command to actuator system. The actuation system of the present system are pumps, non-safety valves, thermal relief valves, emergency relief coupling, emergency shut down valve (Fig.1).

4.2 IDENTIFICATION OF SYSTEM LEVEL HAZARDS, ACCIDENTS AND SAFETY CONSTRAINTS

the main goal of any safety analysis is to keep the system safe avoiding any undesired accident or accidental event. If operation is not performed maintain safe operational boundary, accident may occur. Safety constraints define the requirements or goal which all entities of system should maintain. They may include operational constraint like operational should be carried out within defined limit of pressure, temperature or flow. Safety constraint may also include actions to protect the system from external disturbances or actions to reduce the consequence of accidental event or accident. For the present system, one accidental event is Leak in system. Leak may occu from high pressure, high temperature, high flowrate or external disturbance e.g. high wind, high wave. Moreover, if leak is not controlled, it may lead to fire if ignited. One safety constraint is therefore, ‘pressure should be within predefined limit during operation’. Other safety constraints are e.g. ‘take protective measure to keep the system safe from high wind’, ‘take ignition prevention measure if leak occurs’ or ‘mitigate fire as soon as possible in case of fire’.

4.3 IDENTIFICATION OF REQUIRED CONTROL ACTIONS TO KEEP THE SYSTEM SAFE

Hazardous control actions are identified (Table A.3) by considering each generic mode of unsafe control action. . In this case, one hazard is high pressure in the pipe system which can be reduced by activating a pressure relief valve. The control action here is “Activate Pressure Relief Valve (PRV)”. This can be done by a logic controller, a control room operator or site operator after getting feedback from pressure sensor. Logic controllers can automatically activate PRV when pressure is high. Control room operator can also take action if logic controller cannot take action on time or may notify site operator to activate the valve manually. To execute these processes safety, functionality of sensors, valves, logic controller, availability of electricity, availability of site operators are necessary.

4.4 IDENTIFICATION OF LOW-LEVEL CONTRIBUTING FACTORS OR SCENARIOS

This step is performed to determine how low-level hazard can be eliminated or prevented. Scenarios and causal factors are identified to why and how hazardous control actions can occur (Table A.3). After identifying the low-level causal scenarios, all possible mitigating actions to reduce or mitigate the hazard are identified. For example, to ensure that pressure and temperature does not exceed a defined limit in the system, it is important that they work properly. This can be ensured by designing all valves and sensors to comply with industry design standards and codes and by maintaining them properly.

4.5 IDENTIFICATION OF SAFETY PERFORMANCE INDICATORS

Indicators are identified based on previously developed safety constraint. Further, threshold values need to be defined for each indicator. Depending on the nature of the indicator (whether it is a "positive" or a "negative" indicator), the target may be either to exceed or go below the threshold. Indicators may also have to be seen together. An example may be the two indicators "hours of safety training per person per year" and "average percentage of right answers in the test". If the target is reached for "hours of training", but the "average percentage of right answers in the tests" is below target, it may be argued that the plant should increase quality of training rather than increase number of hours.

4.6 DEVELOPMENT OF PERFORMANCE MONITORING PROGRAM

The resulting list contained 56 indicators (Table A.3), which is a high number considering the limited system. Most of the indicators do not require continual assessment. Indicators which do not need continuous reviewing (e.g. % of periodically verified OSH requirement applied to purchase specifications of machinery, equipment, etc.; no of maintenance check of emergency equipment periodically, % of indicators subject to periodic review and update) are screened out. After screening of established indicators, a shortlist of 14 indicators (Table 1) was chosen as important for continual assessment. One important task of development of monitoring a program is to choose the target value of an indicator. Facilities can set their own value based on practicality, target risk level, additional cost to reach the target, authority requirement and vice versa. An example of target value is for example, in the oil-gas industry SIL 2 rating of safety critical equipment is acceptable. SIL 1 is not acceptable, working hours should not exceed 1800 hours per year, 40 hours per week for onshore.

One indicator is adequacy of documentation. "Adequacy" needs to be specified and defined in such a way that it can be measured. Examples can be the proportion that is in in written form, accessibility by operators and managers and readability. Another indicator is adequacy of training. This can be specified for example by whether the training covers all or specific aspect, % of employees participating the training and % passing the test after doing the course. When the targets are reached, the operator might define more ambitious targets.

The review of safety performance should be a process of continuous improvement. Indicators are intended as a tool for regular (e.g. monthly) review of the condition. This does not mean that performance indicators are a replacement for an audit system. Rather, it is a complimentary activity of more frequent reviewing that enables faster detection of weaknesses and subsequent intervention. The present methodology may be used for development of indicators for all these purposes. Indicators may also be developed and used at all levels in an organisation, such as top management, business area, facility or specific activity. However, the same indicators are not necessarily useful at all levels. Thus, the indicators need to be meaningful at the level where they primarily are being aimed. If indicators are developed for use by operational management, the indicators must be relevant for that level, even if this does not necessarily mean that they are useful and relevant for higher levels in the organisation.

Table 1: Summary of indicators developed by STAMP method

Topic		Indicators	
1	Mechanical integrity	1	Level of reliability of all safety critical equipment including valves and sensors
		2	% of shutdown/isolation systems that functioned to the desired performance standard when tested
2	Documentation and procedure	3	Adequacy of documentation on emergency response action, accident investigation, OSH policies
		4	% of documented history data on equipment and maintenance actions plan
		5	Adequacy of documentation on management of change, organizational changes, change of procedure or equipment including authorisation check, post change check
3	Human resource management	6	Level of competency of personnel for corrosion check, debris check, emergency preparedness, OHS related duties, product transfer, auditing
		7	No of working hours per day or month or year
4	Inspection, maintenance and audit	8	Level of inspection in a year on safety critical instruments, emergency response system, vessel, pipe wall
		9	No of corrective and preventive actions initiated and carried out as a result of audit
5	Risk assessment	10	Level of detail of risk analysis (no of incidents identified, no of incidents not identified, no of unacceptable risk issues)
		11	% of risk reduction actions achieved
		12	No of corrective and preventive actions carried out as a result of root cause analysis of work-related accident, diseases and incidents
6	Training and competence	13	Level of training on emergency rescue action, product transfer, root cause analysis, operational procedure, parameter, automation, corrosion check, prevention, product quality check, change of procedure, auditing
7	Work permit system	14	Level of documentation on work permit issues where the time period for completing the task is specified including hazards, risks and control measures

5 DEVELOPMENT OF OECD AND CCPS INDICATORS

To do a comparative analysis between STAMP based performance indicators and a traditional method used in industry, indicators are also developed by the method described in the OECD guideline and CCPS guideline (presented in Table A.4 to Table A.7). In this paper, outcome and activities indicators are developed for the plant according to OECD guidelines. It is assumed there is a safety management system available in the plant. 100 outcome indicators are developed to check whether the plant has achieved the desired result in establishing a proper safety management system. If these indicators show poor results, a related activities indicator should be evaluated to ensure that the issue is focused appropriately. 38 activities indicators are developed for the present case. CCPS lagging and leading

indicators have also been developed. A total of 17 lagging and 14 leading indicators have been developed relevant to the STS operation.

6 DISCUSSION

In this paper, we have defined safety indicators based on a system engineering approach. LNG ship to ship transfer is chosen as the case study, but detailed process parameters are not specified. For the purpose of illustrating the method, this is considered to be adequate. Developed indicators, considered aspects of system design, can measure safety at the conceptual design. STPA can be started in early concept analysis to assist in identifying safety requirements and constraints. The method can cover possible causal scenarios of accidents including accident prevention design technique, redundancy, barriers, human intervention, use of operational procedures, checklists and training in the analysis. Scenarios can be used to create additional requirements including mitigation or new design decisions.

The developed indicators can be regarded as a mix of leading and lagging indicators. Indicators are leading in the sense that we are giving importance to proactive action before any occurrence of accidents, for example, no of inspection and maintenance checks of shutdown system and no of existing procedures with correct scope and enough detail. Some indicators are also developed based on previous operational records to check any missing barriers in operational procedures or systems. This can be seen as lagging indicators, for example, no of reported flaws in the automated system and no of reported incorrect parameters by operators.

Development of indicators from safety constraints is quite challenging. For example, one constraint is that an operator should be aware of the correct operational procedures. What are the control actions to measure that an operator is aware of correct procedure and can implement them incorrectly? It can be training programs to operators, internal quiz or test to check competency of the operator, and correct documentation which the operator will be able to follow. However, we may still ask if this is sufficient.

Monitoring of indicators established by present method is quite simple, however may become highly human resource intensive.

Indicators based on STAMP are plant-specific while the OECD guidance have predefined sets of indicators. It gives quite an extensive set of indicators, especially in the area of hazard management and personnel safety management. The STAMP-based method focus mainly on operational indicators because it has a clear link to accidental events we want to avoid. All relevant organizational issues can be identified from the causal chain of an accidental event. However, in the case study, the problem is that the system is relatively limited and does not include the whole organization required to operate it. Another benefit of STAMP is that is can be easily modified or revised for any change of plant or system component. For any type of change we need to find the associated hazards, safety constraints and controller actions and performance indicators can be developed accordingly.

If comparison is made with Bayesian belief network, method of developing KPI using Bayesian belief network (Gerbec and Kontić, 2017) requires consideration of direct failures, as well as of factors affecting the events and probabilities and relationship with meaningful safety indicators. Benefit of using BBN model is that level of risk can be quantified. Level of risk reduction, by implementing technological and organizational means, can be quantified also from which management can be benefited.

CCPS lagging indicators considers tier 1 process safety incidents with high consequences and tier 2 process safety events with lesser consequences. CCPS defines industry process safety metrics, so it is easier to make a comparison of incidents in different years and how the plant is running in terms of safety. CCPS leading indicators gives focus to mechanical integrity, action items follow up, process safety training, operating and maintenance procedure and fatigue risk management. Safety management systems developed from CCPS safety indicators will give a total overview of the plant with low effort and cost compared to OECD and STAMP indicators. To consider early warning signs, tier 2 lagging indicators should be given focus.

STAMP indicators are developed from a control hierarchy diagram and gives an abstract of how a hazardous scenario can occur and what safety constraints should be enforced to avoid the hazard. It considers both leading and lagging indicators at the same time. One practical problem related to this model is that a great number of indicators are developed at the first stage. To choose the important indicators from this list is a challenging task. In terms of getting early warning signals, STAMP will be very useful, as even a valve failure or low audibility problem can be identified immediately. So, STAMP can identify errors at the root level. Instantaneous identification of flaws in the plant are possible and so rectifying actions can be taken easily. Threshold values can be used as early warning criteria.

The STAMP model is better than OECD and CCPS in terms of potential for early warning, area of focus, level of details of study, potential to focus on specific issues and ease of modification of model for a change in system. However, this model is still new and industry personnel do not have expertise in how to use it. Low level hazards which do not belong to any class of accidental event and hazardous control actions may have fallen outside the scope of analysis. To improve the sophistication of the study, analysis should include actors, preconditions, alternative processes and non-functional requirements. More study can be done in the future to improve the screening stage, so sufficient control can be achieved with a lower number of indicators.

7 CONCLUSION

This paper presents a method for the development of safety indicators which is based on system engineering. The paper has dealt with three main tasks. The first task is the development of a method for system-based safety indicators, the second task is to apply this to a case study and the third is to make a comparison between the developed method and previously established methods (OECD and CCPS). The method is based on the STAMP accident model. The analysis shows that STAMP-based modelling provides a better understanding of the system. The STAMP-based indicator development process helps to focus on specific issues from which a hazard can evolve. It takes into consideration of human and organization factors along with technical factors to mitigate or prevent high level as well as low level system hazards. Another benefit is that STAMP based indicators can easily be modified or revised for any change of plant or system component. Updating of indicators is easy compared to other processes. In the third part of the analysis, a comparative analysis is presented between STAMP-based indicators program and indicators developed by the methods described by OECD and CCPS. OECD gives an extensive set of indicators especially in the area of hazard management and personal safety management. STAMP based modelling provides better understanding of the system compared to other analysis. Future work can be integration of any risk quantification model with the STAMP model. This integration will support the screening of indicators. Further work is also necessary to investigate to what degree these system engineering-based indicators are complementary to other safety performance indicators or whether they provide a more appropriate measure to foresee unexpected occurrences.

8 ACKNOWLEDGEMENT

The authors wish to thank the Norwegian Research Council and DynSoL AS for their financial support for this project through project no 283861. The contribution of project team members Gisle Obrestad and Kamrul Islam are also acknowledged.

9 REFERENCES

ALE, B. 2009. More thinking about process safety indicators. *Safety science,* 47**,** 470-471.

ANDERSSON, R. & LAGERLÖF, E. 1983. Accident data in the new Swedish information system on occupational injuries. *Ergonomics,* 26**,** 33-42.

ANTONSEN, S. 2017. *Safety culture: theory, method and improvement*, CRC Press.

API, R. 2010. 754 Process Safety Performance Indicators for the Refining and Petrochemical Industries. *American Petroleum Institute, Washington DC*.

BAKER, J., BOWMAN, F., ERWIN, G., GORTON, S., HENDERSHOT, D., LEVESON, N., PRIEST, S., ROSENTHAL, I., TEBO, P. & WIEGMANN, D. 2007. The report of the BP US refineries independent safety review panel, 2007. BP, US.

BENNER, L. 1975. Accident investigations: Multilinear events sequencing methods. *Journal of safety research,* 7**,** 67-73.

BIER, V. M. 1999. Challenges to the acceptance of probabilistic risk analysis. *Risk Analysis,* 19**,** 703-710.

CCPS 2012. Process safety leading and lagging metrics. Center for Chemical Process Safety. AIChE, New York.

CCPS, A. 2007. Guidelines for risk based process safety. Hoboken, N.J.: Wiley-Interscience.

CCPS, A. 2010. Guidelines for process safety metrics. Hoboken, N.J.: Wiley.

CLARKE, S. 2006. The relationship between safety climate and safety performance: a meta-analytic review. *Journal of occupational health psychology,* 11**,** 315.

CLOUGH, I. 2009. The 100 largest losses 1972e2009, large property damage losses in the hydrocarbon industries. MARSH, Global energy practice.

CSB, M. 2007. Investigation report: refinery explosion and fire. *BP Texas city incident final investigation report*.

CSB, O. 2005. refinery and explosion (Giant Industries' Ciniza oil refinery). *Case study, US Chemical Safety and Hazard Investigation Board, Washington, DC*.

DAVOUDIAN, K., WU, J.-S. & APOSTOLAKIS, G. 1994a. Incorporating organizational factors into risk assessment through the analysis of work processes. *Reliability Engineering & System Safety,* 45**,** 85-105.

DAVOUDIAN, K., WU, J.-S. & APOSTOLAKIS, G. 1994b. The work process analysis model (WPAM). *Reliability Engineering & System Safety,* 45**,** 107-125.

DE CARVALHO, P. V. R. 2011. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic management system resilience. *Reliability Engineering & System Safety,* 96**,** 1482-1498.

DOKAS, I. M., FEEHAN, J. & IMRAN, S. 2013. EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety science,* 58**,** 11-26.

EMBREY, D. E. 1992. Incorporating management and organisational factors into probabilistic safety assessment. *Reliability Engineering & System Safety,* 38**,** 199-208.

EPRI 2000. Guidelines for Trial Use of Leading Indicators of Human Performance: The Human Performance Assistance Package. Palo Alto, CA: U.S. Electric Power Research Institute.

EPRI 2001. Final report on Leading Indicators of Human Performance. Washington, DC: EPRI, Palo Alto, CA, and the U.S. Department of Energy, Washington, DC.

ERIKSON, S. G. 2009. Performance indicators. *Safety Science,* 47**,** 468.

GERBEC, M. & KONTIĆ, B. 2017. Safety related key performance indicators for securing long-term business development–A case study. *Safety science,* 98**,** 77-88.

GIBSON, J. J. 1961. The contribution of experimental psychology to the formulation of the problem of safety–a brief for basic research. *Behavioral approaches to accident research,* 1**,** 77-89.

GÓMEZ-COBO, A. 2002. Indicators to monitor NPP operational safety performance. International Atomic Energy Agency, Department of Nuclear Safety, Austria.

GROENEWEG, J., WAGENAAR, W. & REASON, J. 1994. Promoting safety in the oil industry. *Ergonomics,* 37.

GROTE, G. 2009. Response to Andrew Hopkins. *Safety Science,* 47**,** 478.

GUASTELLO, S. J. 1993. Do we really know how well our occupational accident prevention programs work? *Safety science,* 16**,** 445-463.

HADDON JR, W. 1968. The changing approach to the epidemiology, prevention, and amelioration of trauma: the transition to approaches etiologically rather than descriptively based. *American journal of public health and the Nations health,* 58**,** 1431-1438.

HAUGEN, S., SELJELID, J., NYHEIM, O., SKLET, S. & JAHNSEN, E. A generic method for identifying major accident risk indicators. 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, 2012. 5643-5652.

HAUGOM, G. & FRIIS-HANSEN, P. 2011. Risk modelling of a hydrogen refuelling station using Bayesian network. *International journal of hydrogen energy,* 36**,** 2389-2397.

HEINRICH, H. 1931. Industrial Accident Prevention: A Scientific Approach. McGraw Hill, New York.

HENDRICK, K. & BENNER, L. 1986. *Investigating accidents with STEP*, CRC Press.

HSE 2006. Developing Process Safety Indicators—A Step-By-Step Guide for Chemical and Major Hazard Industries. *Health and Safety Executive, UK*.

HOLLNAGEL, E. 2017. Resilience: the challenge of the unstable. *Resilience engineering.* CRC Press.

HOLMBERG, J., SÖDERLUND, T., FORSS, A. & GUNSELL, L. Operating experience feedback by risk based PSA-indicators; Safety and Reliability. Proc. of the European Conference on Safety and Reliability—ESREL, 1998. 16-19.

HOPKINS, A. 2009. Thinking About Process Safety Indicators. *Safety Science,* 47**,** 460-465.

IAEA 2000. Operational safety performance indicators for nuclear power plant. Austria.

JOHANSSON, G. & HOLMBERG, J. 1994. Safety evaluation by living PSA Ð procedures and applications for planning of operational activities and analysis of operating experience. SKI Technical Report 94: 2, NKS/SIK-1 (93) 16.

KHAN, F., ABUNADA, H., JOHN, D. & BENMOSBAH, T. 2010. Development of risk based process safety indicators. *Process Safety Progress,* 29**,** 133-143.

KHAWAJI, I. 2012. Developing System-Based Leading Indicators for Proactive Risk Management in the Chemical Processing Industry Thesis. MIT. June.

KJELLÉN, U. 1984. The deviation concept in occupational accident control—I: Definition and classification. *Accident Analysis & Prevention,* 16**,** 289-306.

KJELLÉN, U. 2009. The safety measurement problem revisited. *Safety Science,* 47**,** 486-489.

KONGSVIK, T., ALMKLOV, P. & FENSTAD, J. 2010. Organisational safety indicators: Some conceptual considerations and a supplementary qualitative approach. *Safety Science,* 48**,** 1402-1411.

LAAKSO, K., HOLMBERG, J., LEHTINEN, E. & JOHANSSON, G. 1994. Safety evaluation by living probabilistic safety assessment and safety indicators. Nordisk Ministerraad.

LEES, F. 2012. *Lees' Loss prevention in the process industries: Hazard identification, assessment and control*, Butterworth-Heinemann.

LEHTINEN, E. & WAHLSTRÖM, B. Safety performance measurement in process industries. Presented at the Third International Conference on Performance Measurement and Management, 2002. 19.7.

LEPLAT, J. 1978. Accident analyses and work analyses. *Journal of occupational accidents,* 1**,** 331-340.

LEVESON, N. 2004. A new accident model for engineering safer systems. *Safety science,* 42**,** 237-270.

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

LEVESON, N. 2015. A system approach to risk management through leading safety indicators. *Reliability Engineering and System Safety,* 136**,** 17-34.

LEVESON NANCY, G. 2011. *STPA: A New Hazard Analysis Technique*, MIT Press.

MARONO, M., CORREA, M. & SOLA, R. Strategy for the development of operational safety indicators in the chemical industry. Proceedings of the 9th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, 1998.

MEARNS, K. 2009. From reactive to proactive–Can LPIs deliver? *Safety Science,* 47**,** 491-492.

MEARNS, K., WHITAKER, S. M. & FLIN, R. 2003. Safety climate, safety management practice and safety performance in offshore environments. *Safety science,* 41**,** 641-680.

MOGFORD, J. 2005. Fatal accident investigation report. *Isomerization Unit Explosion Final Report, Texas City, Texas, USA,* 9**,** 2005.

MURPHY, D. M. & PATÉ-CORNELL, M. E. 1996. The SAM framework: modeling the effects of management factors on human behavior in risk analysis. *Risk analysis,* 16**,** 501-515.

NELSON, P. F., MARTIN-DEL-CAMPO, C., HALLBERT, B. & MOSLEH, A. 2016. Development of a Leading Performance Indicator from Operational Experience and Resilience in a Nuclear Power Plant. *Nuclear Engineering and Technology,* 48**,** 114-128.

NIELSEN, L., SKLET, S. & OIEN, K. Use of risk analysis in the regulation of the Norwegian Petroleum Industry. Proceedings of the Probabilistic Safety Assessment International Topical Meeting. American Nuclear Society, IL, USA, 1996. 756-762.

NIELSEN, D. S. 1971. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis. Danish Atomic Energy Commission, Risoe. Research Establishment.

OECD 2003. *OECD Guidance on Safety Performance Indicators : A Companion to the OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response,* Paris, Organisation for Economic Co-operation and Development.

ØIEN, K. 2001a. A framework for the establishment of organizational risk indicators. *Reliability Engineering & System Safety,* 74**,** 147-167.

ØIEN, K. 2001b. Risk indicators as a tool for risk control. *Reliability Engineering & System Safety,* 74**,** 129-145.
ØIEN, K. 2008. Development of Early Warning Indicators Based on Incident Investigation. Sintef, Trondheim, Norway.
ØIEN, K., MASSAIU, S., TINMANNSVIK, R. & STØRSETH, F. Development of early warning indicators based on resilience engineering. Submitted to PSAM10, International Probabilistic Safety Assessment and Management Conference, 2010 Seattle, USA. 7-11.
ØIEN, K. & SKLET, S. Risk control during operation of offshore petroleum installations. Proceedings of ESREL, 1999. 1297-1302.
ØIEN, K., SKLET, S. & NIELSEN, L. Risk level indicators for surveillance of changes in risk level. Proceedings of ESREL, 1997. 1809-16.
ØIEN, K., SKLET, S. & NIELSEN, L. Development of risk level indicators for a petroleum production platform. Proceedings of the 9th International Symposium of Loss Prevention and Safety Promotion in the Process Industries, 1998. Springer Spain, 4-7.
ØIEN, K., UTNE, I. B. & HERRERA, I. A. 2011. Building safety indicators: Part 1–theoretical foundation. *Safety science,* 49**,** 148-161.
PALTRINIERI, N., ØIEN, K. & COZZANI, V. 2012. Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. *Reliability Engineering & System Safety,* 108**,** 21-31.
PAPAZOGLOU, I. & ANEZIRIS, O. Integrating management effects into the quantified risk assessment of an LPG scrubbing tower. Proceedings of the European Conference on Safety and Reliability (ESREL99), Munich, Germany: Balkema, 1999. 1321ą6.
PODGÓRSKI, D. 2015. Measuring operational performance of OSH management system–A demonstration of AHP-based selection of leading key performance indicators. *Safety science,* 73**,** 146-166.
RASMUSSEN, J. 1997. Risk management in a dynamic society: a modelling problem. *Safety science,* 27**,** 183-213.
REASON, J. 1997. *Managing the risks of organizational accidents*, Routledge.
REIMAN, T. & PIETIKÄINEN, E. 2012. Leading indicators of system safety–monitoring and driving the organizational safety potential. *Safety Science,* 50**,** 1993-2000.
SADEGHI, L., MATHIEU, L., TRICOT, N. & AL BASSIT, L. 2015. Developing a safety indicator to measure the safety level during design for safety. *Safety science,* 80**,** 252-263.
SAQIB, N. & SIDDIQI, M. T. 2008. Aggregation of safety performance indicators to higher-level indicators. *Reliability Engineering & System Safety,* 93**,** 307-315.
SHARP, J., ERSDAL, G. & GALBRAITH, D. Development of key performance indicators for offshore structural integrity. ASME 2008 27th international conference on offshore mechanics and Arctic engineering, 2008. American Society of Mechanical Engineers, 123-130.
TARRANTS, W. E. 1980. *The measurement of safety performance*, University of Michigan-Dearborn.
TINMANNSVIK, R. K. 2008. Building Safety in Petroleum Exploration and Production in the Northern Regions.
THIEME, C. A. & UTNE, I. B. 2017. Safety performance monitoring of autonomous marine systems. Reliability Engineering & System Safety, 159, 264-275.
VINNEM, J. E., AVEN, T., HUSEBØ, T., SELJELID, J. & TVEIT, O. J. 2006. Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. *Reliability Engineering & System Safety,* 91**,** 778-791.
WAGENAAR, W. A., HUDSON, P. T. & REASON, J. T. 1990. Cognitive failures and accidents. *Applied Cognitive Psychology,* 4**,** 273-294.
WINDÉN, B., TURNOCK, S. & HUDSON, D. 2014. A RANS modelling approach for predicting powering performance of ships in waves. *International Journal of Naval Architecture and Ocean Engineering,* 6**,** 418-430.
WREATHALL, J. 2006. Properties of resilient organizations: an initial view. *Resilience engineering: Concepts and precepts.* Ashgate, Aldershot, UK.
WREATHALL, J. 2009. Leading? Lagging? Whatever! *Safety Science,* 47**,** 493-494.
ZHAO, S., SOARES, C. G. & ZHU, H. A Bayesian network modelling and risk analysis on LNG carrier anchoring system. Transportation Information and Safety (ICTIS), 2015 International Conference on, 2015. IEEE, 432-436.