HAZARD ANALYSIS: APPLICATION OF STPA TO SHIP-TO-SHIP TRANSFER OF LNG

Sharmin Sultana[a], Peter Okoh[b], Stein Haugen[a], Jan Erik Vinnem[a]

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

ABSTRACT

The process industry has experienced technological advances, such as automatic handling of hazardous substances, process equipment, and valves. High levels of automation, as well as system interactions at component and system levels, have brought new challenges to risk management. A modern process system involves multiple controllers. Even if each controller can control the process individually, an unexpected event may occur due to unintended interactions or insufficient attention to safety requirements and constraints. Recent accidents in Plymouth, UK, and Nigeria have attracted the attention of scientists, who have concluded that approaches currently being used are insufficient. A traditional hazard analysis tool, such as Hazard and Operability Studies (HAZOP) or simple reliability analysis methods such as Failure Mode and Effect Analysis (FMEA) cannot investigate the lack of complex systems properly. System Theoretical Process Analysis (STPA) is established with the aim of evaluating the safety of such complex systems. It has been used successfully in automated missiles and driving vehicles. However, the use of STPA in process industry applications is scarce. This paper is written to evaluate the feasibility of using STPA in process industry applications. A comparative analysis is conducted between STPA and HAZOP to determine whether STPA can replace traditional HAZOP or not with the help of a case study: Liquefied Natural Gas (LNG) Ship-to-Ship (STS) transfer. The results of the analysis show that STPA is complementary to traditional HAZOP. However, this conclusion is drawn based on only one specific case study (LNG STS transfer) and requires further analysis of other process applications for validation.

1 INTRODUCTION

With the introduction of new technology, modern process systems are facing new safety challenges. Systems have become more software-intensive and are composed not only of hardware components but also logic control devices, software and an increasing number of sensors. Human intervention in certain situations is still unavoidable, and the human-machine interface is always a challenge. In these systems, accidents occur not only due to hardware failure, but also due to software failure, interaction problems between components and controllers (Kletz, 1995; Abdulkhaleq et al., 2017) and error or delay in data entry into the computer.

The BP Deepwater Horizon explosion (Eargle and Esmail, 2012), the fire in the MLGN Tiga project (Mayer et al., 2003), the steam boiler explosion in Skikda Algeria (Ouddai et al., 2012), the LNG accident in Plymouth (WUTC, 2016), and the LNG pipeline explosion in Nigeria (Saheed and Egwaikhide, 2012) have attracted the attention of researchers. They addressed the need for new methods which can eliminate the system flaws related to such accidents. The fire that occurred in the Petronas' LNG complex in the MLNG Tiga project at Bintulu, Malaysia, in 2003 was in the exhaust system of a propane gas turbine. According to the investigation committee, the complexity of equipment, lack of adequate surveillance, lack of integrity of organizational processes and issues with the safety management system (Othman et al., 2014) were contributing reasons for the accident of having adequate inspection plan. In Skikda, Algeria, in 2004, in the LNG production plant, a steam boiler explosion caused a massive vapor cloud including fire.

The accident caused 27 deaths, 74 injuries and damage to a large section of the LNG plant. The accident is reported to have occurred due to poor maintenance, poor site management, lack of accident prevention and improper communication of safety policy (Ouddai et al., 2012). In Nigeria, in 2005, the LNG underground pipeline explosion caused a massive fire that spread over a large area. The accident occurred due to the negligence of personnel during operation or poor maintenance (Khan and Abbasi, 1999). In the investigation of the Plymouth accident, reveals that organizational factors, which the company had not resolved before the accident, were primary contributors. According to Paltrinieri et al. (2015), new disasters require new accident prevention scenarios evolving from innovative technologies, which existing traditional methods are unable to identify. Other recent LNG accidents also draw attention to the fact that human organizational factors, such as miscommunication, lack of integrity of the regulatory process, reduced maintenance, and lack of training for emergency responders contributed to the most of these accidents.

HAZOP (Crawley and Tyler), CHazop, fault tree analysis (Barlow and Chatterjee, 1973) and Failure Mode and Effect Criticality Analysis (FMECA) (Ames Research, 1973), have been used widely for hazard analysis in the process industry for a long time. FMECA evaluates the effect of individual component failures on system performance (Stamatis, 2003). FMECA identifies important causes of failures like component interactions or software errors but does not emphasize the operational context (Stamatis, 2003). CHazop is developed to identify potential hazards and operability problems in control and computer systems. However, a standardized CHazop does not exist. There are various CHazop procedures; yet, none of them have been validated to be considered good engineering practice. CHazop is said to have four technical insufficiencies: Ambiguity, incompleteness, nonsensicality, and redundancy (Hulin and Tschachtli, 2011).

Traditional risk analysis methods assume accidents as a result of component failures or faults (Marais et al., 2004) and oversimplify the role of humans (Leveson, 2011b). These methods are successful in evaluating design flaws in simple linear process systems. For complex interconnected systems, these methods are insufficient and cannot capture the entire accident process (Rokseth et al., 2017). In traditional risk assessment, there is a tendency to assert that designed systems are safe enough, rather than modifying the designed system from a safety point of view (Drogoul et al., 2005). In case of identification of system deficiencies at a later stage, reassessment requires redesign from initial stages, increasing cost and time.

Risk analysis of modern process systems should not focus only on component failure but also software errors, controller interaction problems, and coordination problems in decision making. System-focused risk analysis methods look promising amidst the rapid evolution of technology. Today's risk assessment should include environmental issues, software design error, human error, late decision-making problems, and coordination inadequacy.

Researchers have STPA has been applied in different domains, e.g., security (Young and Leveson, 2014), software safety (Abdulkhaleq et al., 2015), in the aviation industry (Leveson, 2004; Leveson, 2003), the spacecraft design and construction industry (Ishimatsu et al., 2010; Owens et al., 2008; Ishimatsu et al., 2011; Nakao et al., 2011; Chatzimichailidou et al., 2017; Chen et al., 2015), for missile defense systems, and for railways (Dong, 2012). However, process industry application of STPA is infrequent. Two works among them are the work of Hoel (2012) and Thomas (2013). Hoel (2012) has applied STPA and STAMP to process leaks in the offshore industry. He presented a maintenance control strategy for leak detection and mitigation. An extension of STPA has been proposed by Thomas (2013) for nuclear process system.

In the paper of Abrecht (2016), the author shows the advantages of using STPA compared to traditional techniques. According to the author, STPA can identify all the component failures similar to traditional safety analysis. Moreover, it can find additional safety issues compared fault tree analysis or FMECA of the system. Pasman (2015) theoretically explains how STPA can replace HAZOP, FMECA, fault tree and event tree analysis. EPRI (Electric Power Research Institute) ran a comparative evaluation of fault trees, event trees, HAZOP, FMECA, and a few other traditional techniques as well as STPA on a real nuclear power plant design. Experts on the methods applied each hazard analysis technique. STPA was the only one that found a scenario for a real accident that had occurred on that plant design (Fleming et al., 2013).

The work of the present paper is most relevant to the previous work of Rodriguez and Diaz (2016). They have also investigated whether STPA can replace or complement HAZOP in the chemical industry. In their paper, STPA is applied to the lowest level of chemical process and has shown how STPA can be a complement to HAZOP with the help of a case study. They put forward some open questions of using STPA related to the process industry. The questions are how to identify at least one control action for every hazard and how to define system limits from thousands of variables and controllers in the process industry. Further questions are how to choose appropriate states from many states, how to consider many variables and how to cope with process hazard.

This paper aims to apply STPA (System Theoretic Process Analysis) for Liquefied Natural Gas (LNG) ship-to-ship transfer systems, not investigated earlier. The present article tries to examine some issues mentioned by Rodriguez and Diaz, (2016, such as how STPA can consider process hazards like pipe leaks, alarm problems and others, and how to recognize various process variables considered (pressure, flow, composition, temperature and others). In the paper, the "Methodology" section describes the method of HAZOP and STPA. The "Application" section of HAZOP and STPA presents the case study before the results are presented in the "Results" section and discussed in the "Discussion" section. The final section states the conclusions.

2 METHODOLOGY

The present paper describes two hazard identification techniques: HAZOP and STPA. HAZOP is generally used in the planning phase of system development and also in the operational period. STPA uses concepts of system and control theory. It may recognize scenarios which can create a hazard and possibly lead to an accident. STPA tries to identify the measures to eliminate these scenarios by controlling the process.

2.1 HAZOP

The HAZOP technique was initially developed in the 1960s at *ICI* by Kletz and Knowlton to analyze design flaws in chemical process systems. Since then it has been widely accepted and used in the process industries. Other researchers have also developed HAZOP for software (Dunjó et al., 2010; McDermid et al., 1995) and computer systems (Glossop et al., 2000; Andow, 1991; Nimmo, 1994; Hulin and Tschachtli, 2011). The method applies to complex processes for which enough design information is available and not likely to change significantly.

2.1.1 Execution of HAZOP

In conducting the analyses, the HAZOP team divides the whole process into segments based on the process P&ID and identifies essential parameters. Each segment is called a node. Some relevant parameters for a process HAZOP can be flow rate (for liquid flow in a pipe), temperature, pressure, liquid level (for liquid storage in a tank). In the next step, guidewords are chosen (see Table 1) and combined with the parameters to create a deviation. For example, when a guideword “no” is chosen for the parameter "flow," that means the deviation is "no flow” in that node of the system. The team tries to find all possible reasons for and consequences of the
deviation and checks whether appropriate safeguards are present to address the deviation and whether there is any need for further improvement. Causes and consequences are sought for other deviations, for example, "high flow," and "low flow." The HAZOP team repeats the procedure for other relevant parameters: temperature, pressure, level, composition, vice versa. The team then selects the next node and repeats the whole process.
Table 1 shows a standard set of guide words.

Table 1: Possible guidewords of HAZOP

Guideword	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN / INSTEAD	Complete substitution

2.2 STPA

The STPA method was developed by Leveson (2011a) to improve the design of sociotechnical systems. The STPA method was developed based on the STAMP (System Theoretical Accident Models and Processes) accident model. According to STAMP, accidents are more than a chain of events. They involve complex dynamic processes and the result of inadequate control actions. This model considers accidents as a control problem, not just a failure problem, and thus, accidents can be prevented by enforcing constraints on component behavior and interactions.

Three crucial elements of an STPA analysis are safety constraints, hierarchical safety control structures, and process models:

- **Safety constraints**: Safety constraints are criteria that must be enforced on the behavior of the system to ensure safety. According to STPA, hazardous control actions or lack of control actions cause hazardous states system of resulting from inadequate enforcement of safety constraints. Safety constraints are controls that should be implemented to ensure the avoidance of hazards, accidental events or accidents.
- **Hierarchical safety control structure**: This refers to how systems are viewed as a hierarchy of controllers, enforcing safety constraints between each level. The safety control structure of STPA provides an in-depth means for identifying potentially hazardous control actions, by identifying system behaviors and interactions.
- **Process model**: The process model presents how human operators or controllers' function to control the system. The controller should know the present state of the system to manage it, measures to

control and the effect of different control outputs on the network. This statement is true for both automated and human controllers.

2.2.1 Execution of STPA

The STPA method is executed in 5 steps, shown in Figure 1:

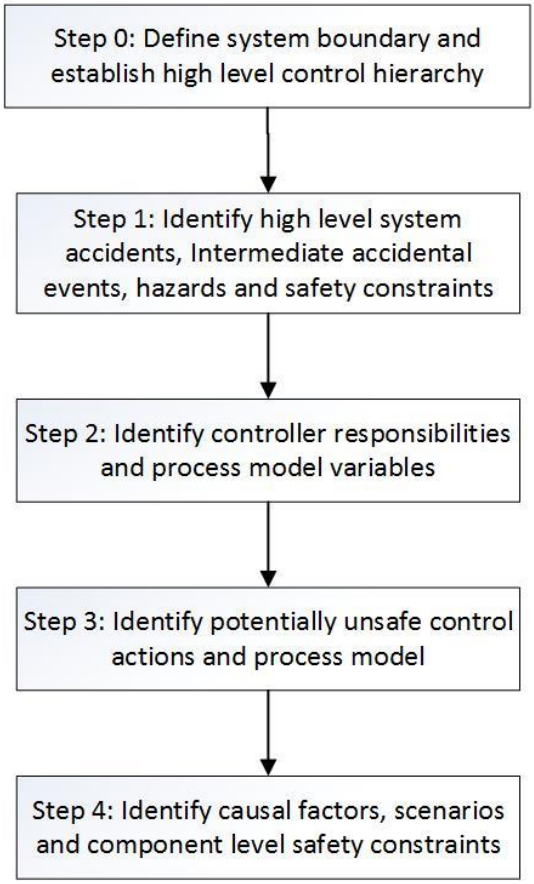

Figure 1: Workflow of STPA

Step 0. Define the system boundary and establish a high-level control hierarchy:

The first step is to define the scope, which is fundamental to any analysis. This step includes conceptualizing the system as a control system and setting the boundary of the system against other entities.

Step 1. Identifying high-level system accidents, intermediate accidental events, hazards, and safety constraints:

This step defines system-level intermediate accidental incidents, accidents, and similar risks. This paper presents system level accidents and hazards as follows:

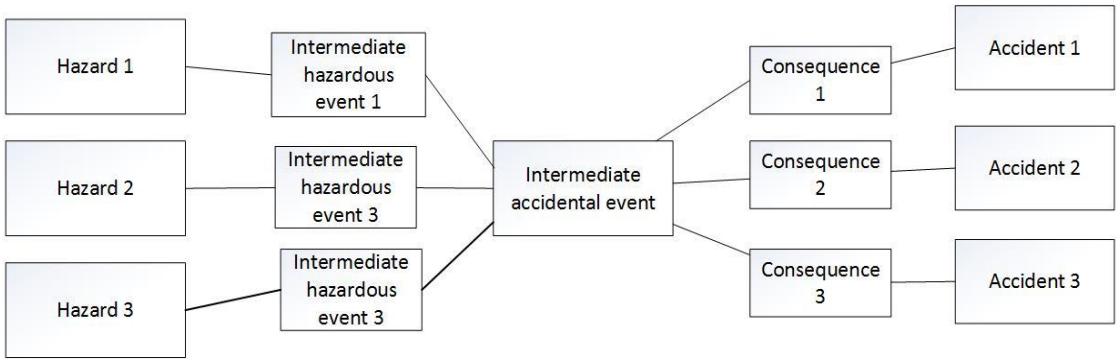

Figure 2: Hazards, intermediate hazardous events, intermediate accidental events, consequences, and accidents

The terms used in the figure are defined as follows:
Hazard: A system state or set of conditions that, together with a set of operational or environmental conditions, have the potential to lead to an intermediate accidental event or accident.
Intermediate hazardous event: Intermediate failures and combinations of failures or events that initiate from a hazard and that are the cause for the next accidental event to occur.
Intermediate accidental event: An event in a sequence of events that upsets normal operations of the system and may lead to an unwanted accidental incident or accident, may require a response to avoid an undesirable outcome and, if not controlled, may lead to undesired accidental events (Rausand, 2013).
Consequence: Effect of any unwanted or intermediate accidental event.
Accident: An aftereffect of an intermediate accidental event which causes harm to people or environment or asset.

An example of an intermediate accidental event is a leak that may be caused by high pressure or high temperature in a pipeline, high liquid level in a storage tank, external wind or wave, a dropped object or corrosion. So, the hazards are high temperature, high pressure or high liquid level in the system. If hazards are not controlled, they may lead to intermediate accidental events (IAE). If IAEs are not controlled, they may lead to several consequences and accidents. The leak may lead accumulation of hazardous material in the process area or dispersion and if ignited may result in fire or explosion or both causing human injury or fatality or product loss or financial loss. The controller can be an operator or logic controller which can control the hazard, preventing an accidental event from occurring.

Step 2. Identify controller responsibilities and process model variables:
It specifies responsibilities and process models for each controller. It influences the next step, where control actions are analyzed. To provide adequate control, the controller must have an accurate model of the process. A process model is used to determine what control actions are necessary to keep the system operating effectively. Accidents in complex systems, particularly those related to software or human controllers, often result from inconsistencies between the model of the process used by the controller and the actual process state (Leveson, 2011). The inconsistency contributes to the controller providing inadequate control. Usually, these models of the controlled system become incorrect due to missing or insufficient feedback and communication channels.

Step 3. Identify potentially hazardous control actions and process models:
Identifies the potential for inadequate control of the system that can lead to a dangerous state. According to Leveson (2011), hazardous states result from inadequate controls or enforcement of safety constraints, which can occur because:

1. A control action required for safety is not provided, or not followed
2. A hazardous control action is provided
3. A potentially safe control action is provided too early or too late, or in the wrong sequence
4. A control action required for safety is stopped too soon or applied too long

A control action by itself does not provide enough information to determine whether it is safe or hazardous. Additional information is necessary, including the context of the environment. Considering each responsibility of each controller can identify potential hazardous control actions for a system.

Step 4. Identify causal factors, scenarios, and component-level safety constraints:
Determine how each of the hazardous control actions could occur by identifying causal factors and scenarios. This goal is achieved by investigating each element of the control loop or control hierarchy and assessing whether any of the elements could cause the hazardous control actions in question. After identification of scenarios and causal factors, one can identify safety constraints. Safety constraints keep the system from hazardous states or mitigate the consequences.

3 Application of HAZOP and STPA to STS Transfer of LNG

In this section, HAZOP and STPA have been applied to the LNG STS (ship-to-ship) transfer system. The intention is to demonstrate how hazard analysis can be accomplished for the system, using the two methods. The considered system is as generic as possible.

LNG STS transfer for offshore systems is the transfer of LNG from or to an LNG carrier vessel (LNGC) to or from an LNG storage ship or floating storage and regasification unit (FSRU). With increasing demand for energy, LNG ship-to-ship transfer has increased to supply low cost liquefied natural gas to remote areas where local energy resources are scarce. The transfer is done using high-pressure pumps. The consequences of loss of containment during this operation can be severe. The traditional method of risk analysis for these types of systems is HAZOP (Crawley and Tyler, 2000), where the objective is to improve the design to establish a safe design.

3.1 System description

STS transfer of LNG is carried out in port. After arrival and mooring of an LNG cargo ship, required tasks include inserting the LNG transfer line, checking storage tank systems and related equipment, earthing, connecting hoses & links, opening the manual and automatic valves and, finally, starting the pump. After completion of the liquid transfer, operators stop the pump, purge the lines, and disconnect the hoses. It is essential to follow the sequence to ensure the safe and proper execution of the transfer.

The main component of the STS transfer process is the pump. Other vital components include control valves, motors, hoses, and pipelines. During operation, flexible pipes from the storage tank of the carrier ship are connected to the storage tanks of the storage ship by manifold. Motors can control the speed of the pumps, and valves are used to control or regulate the flow of liquid. Thermal relief valves are installed with pipes to control temperature or pressure of the fluid. Emergency relief valves or

emergency relief couplings are connected to stop liquid transfer or disconnect the pipe during an emergency. The pump creates a pressure difference between both ends of the pipeline to establish the desired flow. The function of the electrical system is to provide energy to operate the motor driving the pump. Thermal relief valves are installed to reduce pressure or temperature effects on the network. These can be controlled automatically or manually. For the actuators to perform the commands, an adequate amount of power must be available. In this analysis, we do not specify any power system solution to keep the study generic.

Modern process systems are equipped with logic controllers or programmable controllers, by which all the components, like pumps and valves, can be controlled. Control room operators can observe all operations of the plant to ensure everything is working correctly. Figure 3 presents a simplified process flow diagram. It is common practice to apply top filling, to reduce the pressure in Tank 2. Excessive pressure may make the pumps work harder. Transfer speed ranges from 100–1000 m3/hr, depending on the scenario, tanks, and equipment. This rate can be altered during transfer to reach a pre-established amount. Both ship authorities can monitor conditions of the transfer, e.g., system pressure, tank volume, and equipment behavior. To start the transfer from *Tank 1* to *Tank 2*, *valves V3, V4, V7, V8, V11, V12, and V15* must be opened.

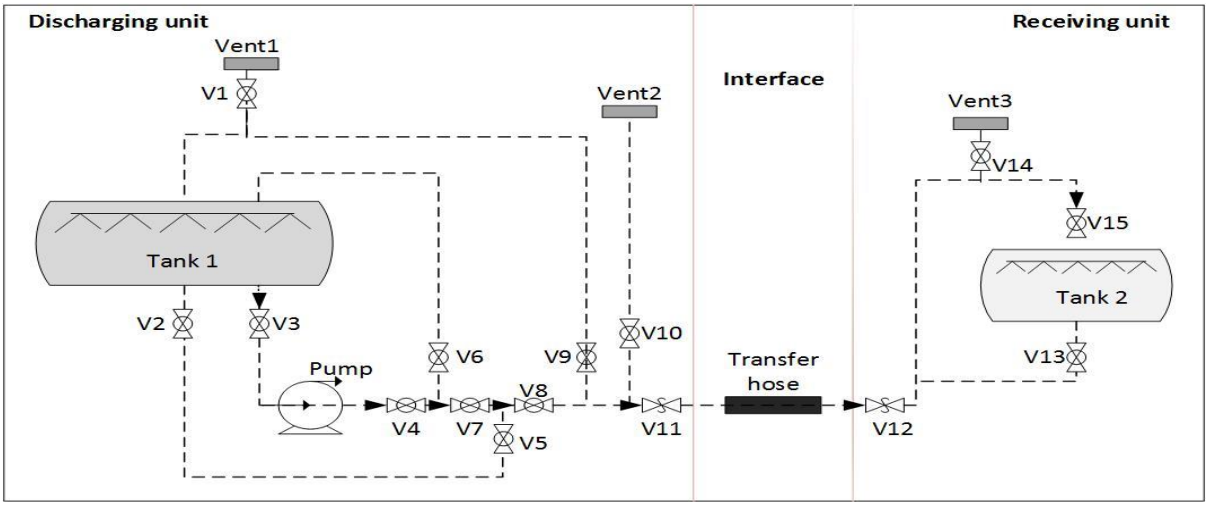

Figure 3: Process sketch of LNG ship-to-ship transfer procedure

3.2 EXECUTION OF HAZOP

Before the execution of HAZOP, HAZOP team specifies the specific nodes from the P&ID. Control lines are in dotted line in Figure 3. Arrow lines show the route of liquid flow. The team choses one node first. Next, they search for appropriate parameters and guide words. The present case uses parameters like flow rate, pressure, temperature, composition, and liquid level. It also uses additional parameters related to operational safety, (e.g., service failure, maintenance, abnormal operation, information). Guidewords chosen are "High," "Low," "No," "Reverse" and others. The team searches for possible causes and consequences for each deviation. For example, what are the causes of “High temperature," and what might be the consequences? Recommendations are made to avoid the deviation "High temperature” and the possible consequences of the deviation. Table 2 shows part of HAZOP worksheet.

Table 2: HAZOP for LNG transfer (part of)

Parameter	Deviation	Causal factors	Consequences (system reaction)	Actions required
Flowrate	1.1 High	Ship pump malfunction, control valve malfunction, PLC failure, undefined procedure, boundary conditions, threshold value, valve fully open due to debris, debris suddenly loosened	High level in the tank, High flow over a period may cause flow-induced vibration, may cause pipe rupture and leakage	Consider flow meter and high-level alarm if not previously identified, clarify design basis
Pressure	2.1 High	PCV failure, an inadequate volume of vents, external fire, weather condition, changes in density, external fire	Fire, explosion, fluid loss, water hammer on site, rupture of the pipe	Assess risk and redesign pressure protection system Adjust PSV set points, implement new shut down functions, improve the reliability of shut-down functions, improve the operational procedure
Temperature	3.1 high	The ambient condition, fire situation, defective control valve, internal fire, faulty instrumentation and control, cooling system failure, mechanical heating	LNG loss via a relief valve	Improve the reliability of thermal valves
Composition	4 Abnormal contamination	Bad LNG quality from ship, leaking isolation valves, incorrect operation of the system, ingress of air, ingress of water, corrosion, gas entrainment	LNG inside tank polluted, corrosion or erosion inside the pipe	Check design basis against operational experience
Concentration	5 Low	Impure raw material, leak in the line, phase change, process control upset, gas entrainment	Performance of equipment gets affected, contaminated product, chances of severe working conditions	Check material quality
Level	6.1 high	The ship does not stop unloading (operator mistake or pump malfunction), outlet isolated or blocked, faulty level measurement, corrosion, pressure surge, Wrong level information (sensor problem), leakage on the storage tank	Fluid leakage on PRV due to a pressure increase	Install reliable level sensor Take protection for corrosion, blockage
Service failure	7	Electric power, water supply, telecommunications, PLCs/computers, HVAC, fire protection, steam	Abort of operation	Check for an alternative arrangement of electricity, water.

3.3 EXECUTION OF STPA

3.3.1 Define system boundaries and establish a high-level control hierarchy (step 0)

This step defines the STS system boundaries and establishes a high-level control hierarchy. *Figure 4* shows the high-level control structure of an STS transfer system. The system consists of three controllers, actuator systems and disturbance processes (wind, waves and current). Three kinds of controllers are logic controllers (also called auto controllers), control room operators and site operators. The objectives of the controllers are to induce the desired flow of liquid in the pipeline by providing suitable commands to actuators and to protect the system from external disturbances. Actuators and disturbances affect the STS process. The control hierarchy diagram (Figure 4) provides the means to communicate between developers, analysts, and users. It also includes other relevant information.

The logic controller (or programmable controller) is a digital computer which can control the process equipment such as the speed of pumps and motors, opening or closing process or safety valves, vice versa. Control room operators can control some equipment or states of the system. For example, the flow of electricity and the opening or closing of valves by getting feedback from the sensors attached to the system. In process systems, the site operator has an important role. He (or they) monitors the plant during a site visit and takes appropriate actions. In cases where the automatic controller cannot act, or the control room operators cannot fix the problem, they are responsible for setting the problem manually since they are physically present.

The actuation system is composed of pumps, non-safety valves, thermal relief valves, emergency relief coupling, and emergency shutdown valves (see *Figure 3*). For automatic control, they get commands from logic devices to go into the position of "open" or "closed" to relieve thermal energy into the environment. The logic device determines this requirement from the feedback of sensors. Here, we consider each component not only as a component of the system but also as an actuator of the system which can control the operation.

3.3.2 Identification of system-level hazards, accidents, intermediate accidental events and safety constraints (step 1)

To keep the system safe, we want to avoid system-level accidents and unwanted intermediate accidental events. First, we define system level accidents and adverse intermediate accidental events and their related hazards. There can be many accidental events which lead to an accident. From the *Hazards and Accidents List*, we define safety constraints to avoid them. " One important aspect of the analysis is to follow the control objectives. Control objectives depend on the function of the system in the operational context. In this case, the control objective is to make the liquid flow within the defined limit. Accidents or hazards may occur if control objectives are not followed or are not suitable to the operational function of the system. System-level safety constraints can be derived directly from the hazards and should include constraints to *avoid* accidents. For the present case, one accidental event is "Leak in System". Table 3 summarises system-level safety constraints related to leakage in the system.

3.3.3 Identification of process model variables and controller responsibilities (step 2)

This step defines process model variables from the high-level safety constraints. Process model variables are those parameters in a system that need controller action to keep the system operating safely. Process model variables can identify controller responsibilities. Different responsibilities of each

controller in the control hierarchy need to be defined to identify hazardous control actions. In STPA, each responsibility, or each specific control action derived from the responsibilities, is considered concerning whether it can cause inadequate enforcement of safety constraints. Table *3* shows process model variables for each high-level system hazards and accidents.

3.3.4 Identifying hazardous control actions and process model for the control actions (step 3)

In this step, we use the control actions and process model variables to identify hazardous control actions. *Table 4* presents the hazardous control actions identified for an accidental event of leakage in the system. Analysts identify hazardous control actions by considering each generic mode of unsafe control and relevant process model variables. Later, we establish the process model to determine the circumstances requiring hazardous control action. From the process model, we can see controller actions, responsibilities, and entities giving feedback to controllers and actuators involved to execute one single control action. In this case, one hazard is high pressure in the pipe system, which can be

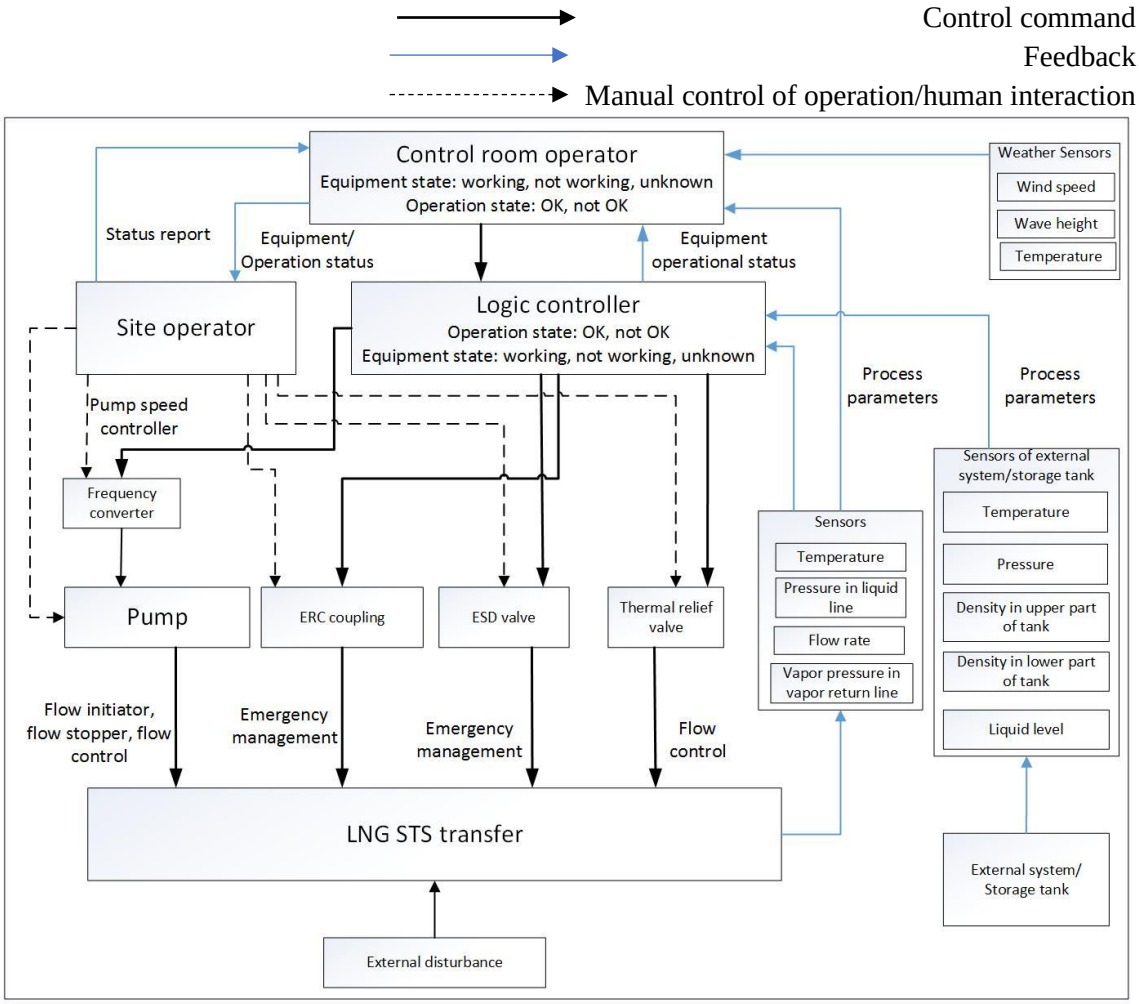

Figure 4: High-level control diagram of LNG STS transfer

reduced by opening a pressure relief valve. The control action here is "Activate Pressure Relief Valve". A logic controller or a control room operator or a site operator can execute the action. A pressure sensor attached to the pipe system gives feedback to the logic controller, which is visible to the control room operator also. The site operator can see the sensors physically. Table 4 presents hazardous control actions. The process model helps to identify causal factors and scenarios. An example of a process

model is shown in Figure 5, how a pressure relief valve works to control the process. The sensor gives feedback to the logic controller when there is high pressure in the system. The logic controller can give the command “open” or “close” to pressure relief valve to relieve pressure. The control room operator can be aware of the state of operation and can give a command to the logic controller to act or can inform the site operator to take action when the logic controller cannot control the system automatically.

Table 3: High-level system hazards, safety constraints, process model variables and possible control actions in the process for each intermediate accidental event (part of)

Intermediate accidental event: ‘Leak.'			
High-level System hazards	**High-level Safety constraint**	**Process model variables**	**Examples of control actions**
H1: High pressure in the system	The pressure in the system should not exceed a defined limit The temperature in the system should not exceed a specified limit A fire that occurred nearby should not affect the system	High pressure in the system A high temperature in the system	Activate pressure relief valve Activate process safety valve Extinguish fire Check insulation on the pipeline
H2: Low pressure in the system	The pressure in the system should not be below a defined limit	Low pressure in the system Pump speed	Check pressure control valve Check vent valve Regulate pump speed as desired Check for a leak in the system Protect system against leakage
H3: High temperature in the system	The temperature should not exceed a defined limit The pressure in the system should not exceed a specified limit A fire that occurred nearby should not affect the system	A high temperature in the system High pressure in the system	Activate pressure relief valve Protect the system from sunlight Extinguish fire Check insulation on the pipeline
H4: Low temperature in the system	The temperature in the system should not be below a defined limit	Low temperature in the system Low pressure in the system	Check for a leak in the system Check pipeline insulation
H5: Liquid level exceeds the high limit of the storage tank	The liquid level should not exceed a defined limit	Liquid level high	Stop the pump
H6: High flow rate in the pipe	Flowrate should not exceed a specified limit	High flow rate	Control flowrate Check pump functionality Check valve functionality Check the pipe network for debris
H7: Low flow rate in the pipe	Flowrate should not be below the defined limit	Low flowrate	Control flowrate Check pump functionality Regulate pump speed as desired Check valve functionality Check the pipe network for debris Check pipe network for leak

Table 4: Hazardous control actions (part of)

No	Control action/event	Control action not provided causes hazard	Control action provided when not required causes hazard	Control action provided too early causes hazard	Control action provided too late causes hazard	Control action stopped too soon or applied too long
1	Open PRV	PRV valve is not activated when pressure/temperature exceeds the high limit	PRV opened when pressure/temperature is within range	N/A	PRV/PSV is opened too late after detection of high pressure/temperature	N/A
2	Mitigate fire	The fire protection system is not activated when there is fire	The fire protection system is activated when there is no fire	N/A	The fire protection system is activated too late when there is fire	Fire protection system gets off before the fire is mitigated
3	Check insulation on the pipeline	Missing pipeline insulation check and insulation protection is absent	N/A	N/A	N/A	N/A
4	Check valves functionality	Regular maintenance check on the valves is missing	N/A	N/A	N/A	N/A
5	Regulate pump speed as desired	Pump speed cannot be regulated as desired	N/A	N/A	N/A	N/A
6	Check for a leak in the system	Check for leakage in the system is missing	N/A	N/A	N/A	N/A
7	Protect system against leak	Leak protection measures are missing	N/A	N/A	N/A	N/A
8	Protect the system from sunlight	The sunlight protection system is absent	N/A	N/A	N/A	N/A
9	Control flowrate	Controllers cannot control the flow rate when the flow is not within range	N/A	N/A	The flow rate is controlled too late when the flow is not within range	N/A

Table 5: Causal factors and low-level safety constraints for each hazardous control actions (part of)

Hazardous control actions	**Causal factors**	**Low-level safety constraints**
Controllers cannot activate the pressure relief valves when pressure/temperature exceeds the high limit	1. Pressure sensor failure 2. Pressure relief valve failure 3. Communication error 4. Auto-activation is turned off 5. The problem in decision-making arrangement 6. Electricity blackout 7. The operator is reluctant to act due to high workload 8. Poor audibility/visibility of sensor 9. The operator is confused to follow the procedures	1.1 Sensors must be designed to operate for X years with no defect 1.2 , 1.3 There should be a maintenance program to test the sensors after Y year 1.4 , to replace after Z years 2 There should be a check of valves after every Y year 3 Good communication arrangement between control room operators and site operators 4 Mode of each system/component should be defined clearly 4.1 The operator should know in which mode each component is working 4.2 The operator should know the exact control actions to be performed by auto controllers or not 4.3 Operators should know the timeframe within which auto controllers need to activate and maximum allocated time until controllers take action 5 Alternate energy source should be available 6 Operator's maximum working time should e followed according to regulation 7 The maintenance program should be established to check the audibility/visibility of sensors before starting operation 8 Should be trained for operating each component and valve manually
The pressure relief valve is activated when pressure is within range	1. Pressure sensor malfunction 2. Communication error	Mentioned earlier
Fire suppression system is not activated when a fire is detected	1. Detector malfunction 2. Communication error (missing signal) 3. The operator is reluctant to act due to high workload 4. Poor audibility of the detector 5. The operator is confused about the procedures	Mentioned earlier
Fire suppression system is activated when there is no fire	1. Detector malfunction 2. Communication error	Mentioned earlier
Missing pipeline insulation check and insulation protection	1. The job is out of scope in the maintenance log 2. The operator is reluctant to perform the task 3. Lack of operator training	1. Update maintenance log regularly 2. Follow the standard working time of an operator 3. Provide adequate training and trainer to operators 4. Provide well-insulated pipe

3.3.5 Identifying causal factors and scenarios (step 4)

After identifying hazardous control actions in the previous step, this step identifies potential causes and their preventive measures. Accidents can occur by any action which is not hazardous directly but creates a hazardous situation. For example, if controllers provide appropriate safe action, but in the wrong order or using the wrong procedure, it may lead to an accidental event or accident. Overall, the step tries to identify violations of safety constraints or how they can occur (scenarios). Scenarios can be determined to enhance knowledge about why and how hazardous control actions can happen, and associated causal factors. Table 5 presents causal factors for hazardous control actions.

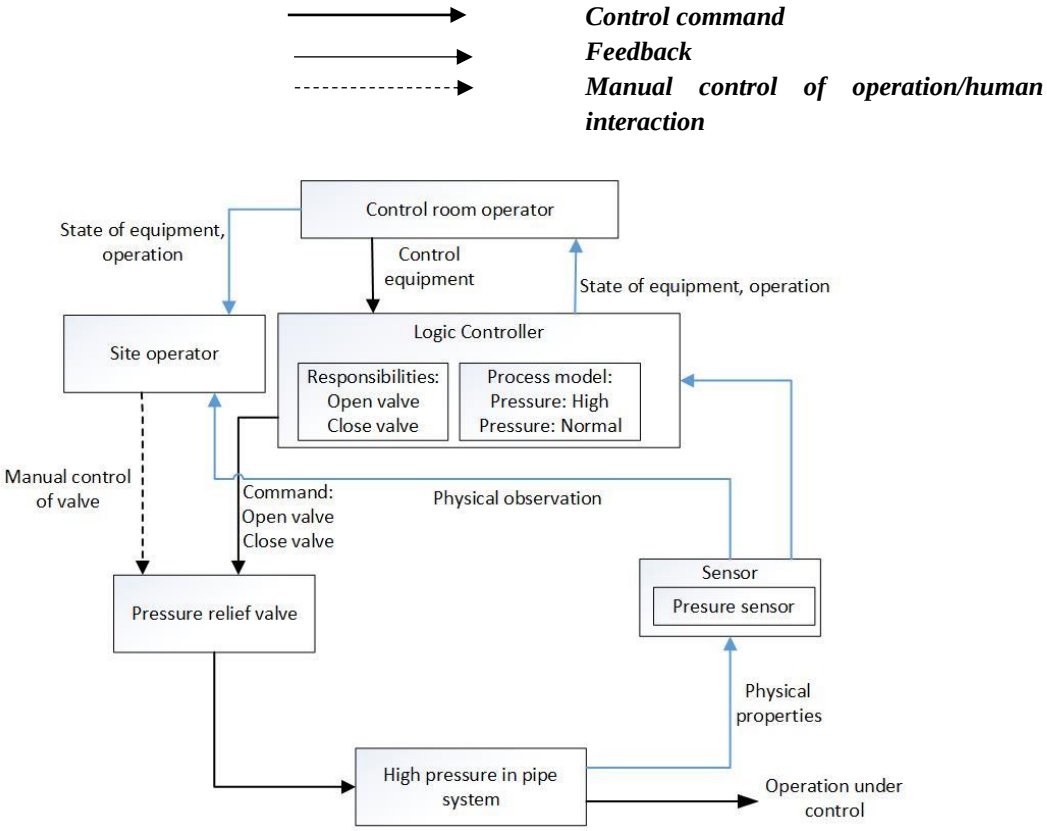

Figure 5: Process model to control pressure in LNG transfer system

Table 6: Comparison between HAZOP and STPA (part of)

Hazard category	**Identified by HAZOP? Examples**	**Identified by STPA? Examples**
Component error	Ship pump malfunction Sensor malfunction PRV/control valve/check valve failure Logic control failure Vent valve open Low audibility/visibility of sensor	Ship pump malfunction Pressure or level sensor malfunction in functionality, audibility or visibility Detector failure Control equipment malfunction Emergency rescue equipment malfunction Fire suppression system malfunction
Organizational error	Operators did not follow the unloading procedure mentioned in the protocol	An alternate system is not available during maintenance due to lack of redundancy or planning The organization does not follow a standard working time of operators

Hazard category	**Identified by HAZOP? Examples**	**Identified by STPA? Examples**
	Ignorance about operational boundary (Flow, Pressure, Temperature) Ignorance about the operational condition (empty tank, pressure, temperature, level)	Lack of a healthy working environment Lack of a well-documented operational procedure Insufficient preparation before the operation Lack of well-trained resource, Lack of training about equipment handling, emergency rescue action, corrosion check, leak check Lack of communication between interdisciplinary team Lack of satisfaction of workers about workplace, salary or facility provided Wrong decision making by managers in the operational procedure Missing regular update of maintenance log, Low reliability of equipment or instruments Insufficient redundancy of equipment Poor planning of the operation, Lack of existence or implementation of accident prevention strategy (high wave, wind, ignition, dropped object) Lack of operators' safety procedures
Human error	Valve half closed/entirely closed during operation Bad LNG composition, Debris in the pipeline External Water/particles inside the product Remaining pressure in line The operator gives the wrong command More injection of wax/scale inhibitor Wrong operational procedure Incorrect information about pressure, temp, level	Operator not aware of the operating condition or system condition or instrumentation malfunction or product quality Missing action of the operator due to high workload or dissatisfaction about work Wrong operation of an operator Wrong operational procedure The late arrival of the emergency rescue team Maintenance log is not updated regularly Poor insulation of pipe or product quality check
Software error	Valve half closed/entirely closed during operation	Wrong voting arrangement Bug in software, Intentional sabotage or hacking of software
System or design error	Electricity blackout Leakage in pipeline Internal leakage in valves Overpressure/ overheating due to fire/PRV failure Insulation failure Liquid accumulation in line, Remaining pressure in line An unwanted shutdown of the system Missing emergency rescue action, Flow-induced vibration Local instrument missing	Electricity blackout, Communication error Leakage in pipeline Overpressure/ overheating of equipment Insulation failure Missing emergency rescue action Poor or missing insulation of pipe The system is not protected against the high wave, wind or dropped object Logic control system malfunction
External events		The system gets affected by wind, wave or dropped object.

4 DISCUSSION

This paper makes a comparison between two hazard identification processes, HAZOP and STPA. LNG STS transfer process has been chosen to investigate the feasibility of the application of STPA for a modern process plant that requires human intervention to a large extent, which is a characteristic of a sociotechnical system. Table 6 presents a comparative analysis. The analysis of the present case study shows the effectiveness of STPA as declared.

To conclude that STPA can replace HAZOP, it must cover all the functions of HAZOP. To say that STPA can be complementary to HAZOP, it should provide an improved risk picture if performed. It should demonstrate the issues which are not covered by HAZOP but can be covered by STPA. The authors of the present paper classified the identified hazards from the analyses into the following five error categories:

- Human and organizational errors
- Software errors
- Component errors
- System errors
- External events

The two methods are compared based on these error categories. Other qualitative criteria are discussed later, i.e., documentation requirements, time requirements, resource requirements, level of detail, confidence in results and applicability.

4.1 HUMAN AND ORGANIZATIONAL ERRORS

The case study results show that STPA can cover more organizational errors. The results are almost the same for both cases in the identification of human errors. Human HAZOP or human factors (HF) HAZOP are being used nowadays to analyze human interaction or involvement. Different guidewords are used then such as ‘no action taken,' ‘action was taken later,' ‘more action was taken' to conduct human HAZOP. The present case study performs a traditional HAZOP and makes a comparison with STPA based on that. The parameters used in the case study are identical to those used in the conventional HAZOP. It is challenging to identify organizational deficiencies in a HAZOP compared to STPA. The reason for this is that HAZOP was developed to find deviations caused by the system in the process industry, not to find deviations in human action or organization. STPA uses a hierarchical control diagram to show the whole system along with its interaction with other components, and their effects on the network. As it uses a systematic process to identify safety constraints, organizational deficiencies and requirements can be included, something which is not possible in traditional HAZOP. Moreover, the control hierarchy established in the paper for STPA does not cover much of the organization "above" the operation. Extended structure could have been found more deficiencies.

4.2 SOFTWARE ERROR

Identification of software error requires a good understanding of software behavior, interactions and effects on other systems. HAZOP is less efficient in the treatment of software error because both hazardous and non-hazardous data flows must be analyzed. The presence of complicated software limits the use of classical techniques. By applying a combination of traditional HAZOP, HF HAZOP and Software HAZOP, more hazards could have been identified, but this requires further work.

4.3 COMPONENT ERROR

The results are almost the same for identifying component errors. HAZOP has proven to be a useful tool for identifying and evaluating component-related hazards associated with the processes utilized in the hydrocarbon and chemical industries. The fact that STPA produces very similar results indicates that this method is equally valid. HAZOP is considered suitable for identifying hazards arising from single, independent contingencies.

4.4 SYSTEM ERROR

HAZOP can identify any deviation in the system quickly. We do not explicitly mention the environmental conditions of execution. System safety is built into the design to ensure that, for each deviation in a process parameter, at least two levels of safeguards protecting against deviation and operator actions are included (Goyal, 1993). In STPA, success, however, depends on proper identification of intermediate accidental events. Low-level hazards which do not belong in the class of any accidental events and hazardous control actions may have fallen outside the scope of analysis. We should include actors, preconditions, alternative flows and non-functional requirements in the study to mitigate for this.

4.5 EXTERNAL EVENTS

In STPA, using the control hierarchy diagram, the effects of external events can be identified conclusively in a systematic way. HAZOP is also able to determine the outcomes. However external events are traced in an unsystematic way, which gives an uncertainty of the completeness of the analysis to consider all the event.

4.6 DOCUMENTATION REQUIREMENTS

HAZOP is performed based on the process flow diagram (PFD) or P&ID, developed at the design stage. STPA examines the essential functions of each entity in the control loop and requirement for effective safety system behaviors. One can redefine goals and related system performance and may develop alternatives for analysis. This approach emphasizes the importance of the process model in enforcing adequate control. System behavior is expressed in relationships that represent the structure of the system in a hierarchical control model. One can work with STPA with a primary process flow diagram (PFD) before establishing the detailed process and instrumentation diagram (P&ID).

4.7 TIME REQUIREMENTS

This criterion relates to how time-consuming the methods are to apply to a specific application. The industry is using HAZOP for a long time. Industry personnel is well known of the method and execution process. The method is also straightforward, and those not familiar with it usually understand it very quickly.

On the other hand, STPA is quite a new method and has not been implemented for many systems, especially the process industry applications. Industry personnel may find it difficult to execute. Identification of causal factors and step-by-step execution can be challenging. Including the system study, the analysis time required for STPA was three times longer than the time needed for HAZOP for this study. This negative aspect of STPA may indicate that it should be used not necessarily for complete process systems but for more limited parts of the system, which are particularly challenging to analyze with HAZOP.

4.8 Resource requirements

To conduct a HAZOP, experts from all disciplines need to participate face to face and check the deviation. Feedback from all discipline experts is considered to find the deviation, e.g., electrical, automation, instrumentation, software, process. Resource requirement is the same in case of STPA.

4.9 Level of details

HAZOP follows a deductive or downward approach like top events and deviations and tries to find what would happen to the system due to the deviation. This approach is easy to follow and has made HAZOP widely accepted for the analysis of systems (Hoepffner, 1989). However, this type of analysis becomes difficult when the boundaries of the study are too vast, and guidewords become too numerous. There is no systematic method to limit the guide words. HAZOP identifies causes of deviations but does not usually go into detail analysis of causes. STPA, in general, can go into details in deriving causes of failures in a better way. Its step-by-step and systematic approach assures identification of all potential hazards. Users can refine every hazard and safety constraint at the lower level and can go into the details of each issue of system requirements. However, for process industry applications, to set the boundaries of study, to find the required number of variables to be studied, the required control actions for each safety constraint, and the role of controllers for each control action needed (CA) in STPA are also challenging. The process industry uses thousands of variables, and they can be in various states (online, offline, in maintenance).

4.10 Confidence in results

The confidence of decision-makers in the analysis and its effects are a considerable factor in decision-making. In this respect, HAZOP has an advantage since it is a well-known method that has been shown to work for decades, while STPA is quite a new method. Risk assessment may help people evaluate the risks they face. Information is needed to identify those risks to take precautionary measures. People have more confidence in studies that are in line with prior beliefs. In the case of a new method, the user may not find the confidence to use it, even if it is superior. In STPA, the user may get confidence from its level of detail. However, the success depends mainly on the proper establishment of a functional control diagram. A disorganized functional control diagram may lead to an incomplete result and completely unuseful analysis. On the other hand, a well-organized functional control diagram is the most significant strength of STPA.

4.11 Applicability in a specific application

The final criterion is to assess how applicable the analysis is to identify different types of hazards in various industry. From the comparative analysis (*Table 6*), STPA is shown to be more capable of identifying organizational error and effects of external events. The case study chosen here is for a simple system. The result became very similar in case of the two analyses. Possibly, results may become significantly different for a more complex system. STPA would be more suitable to apply for a complex system as it tries to find the hazards in a very systematic way. The challenge of STPA would be to deal with many variables and controllers, the number of state variables, the number of variables and above all defining the system limit (Rodriguez and Diaz, 2016).

Moreover, for complex systems, the time required to conduct STPA may become very long compared to HAZOP. That is a significant disadvantage of STPA. However, the longer time can be justified as STPA provides a more detailed analysis and takes a short time for future modification of the plant.

The findings of the paper confirm the results of the article by Rodriguez and Diaz (2016) that the differences between both techniques are not very important at the lowest level. The advantage of using STPA is that the analysis is very systematic and very suitable to apply for a sociotechnical system. STPA requires one single study to be conducted to cover all aspects of errors. One can readily design the mitigation strategy and can evaluate their effectiveness from control algorithms through scenario analysis. STPA can capture the dynamic behavior of systems. The root scenario can be used to communicate the need for mitigation strategies at board levels. The control diagram describes the faulty or malicious system behavior at a high level and points out the potential system losses.

Industry uses a combined approach, HAZOP for hazard identification and SIL (Safety Integrity Level) for risk analysis. They use other assessments on a case-by-case basis, e.g., human factor, system reliability, CHAZOP. CHazop can be overwhelming when performed on a complex software system with large quantities and varieties of data flow. In the case of a process-oriented control system with very little flow of information but with a complicated control algorithm, the data flow may not be the right unit of analysis (Thomas, 2013). HAZOP relies on user's understanding of software behavior, interactions and effects on other systems.

Compared to a traditional human factor model, in STPA, scenarios and causal influences are easy to identify using the human controller model as a starting point. It can address issues related to human-automation interaction before the final automation design finalized. The role of the human operator on system operations can be analyzed, and design can be modified accordingly. Unlike the automated controller, the human has a control-action generator rather than a fixed control algorithm. One advantage of having a human in the loop is the flexibility to change procedures or create new ones in a situation.

5 CONCLUSION AND FUTURE WORK

The objective of this article has been to assess the feasibility of using STPA for hazard identification in automated process systems and determine whether STPA can replace traditional HAZOP or become complementary to HAZOP. A specific process system, a ship-to-ship transfer system for LNG is used to perform the analyses and to make the comparisons. The study shows that the causes identified by STPA and HAZOP are almost identical. Potential causes identified by STPA cover hardware failures and communication errors, including delayed communication and software errors, which is the case for HAZOP also.

The results show that STPA is a systematic hazard analysis technique that provides systematic guidance and recommendations for safety requirements. The primary challenge in STPA is to establish the control structure. However, the process of developing the control structure is a beneficial process because it provides additional insight into how the system works, in particular, on the higher level of the hierarchy. For complex systems which involve highly automated systems and many interactions of components, STPA can be applied to understand the system's behavior. It ensures the completeness of the hazard list and can link different control structure diagrams from a high level to a detailed level. For any process system that involves simple interactions and less software, HAZOP can be more suitable, considering its simplicity and lower time requirement. Authors draw the conclusion based on the present case study. Other additional case studies may provide further perspectives on the use of the method.

The present paper tries to solve some questions raised earlier (Rodriguez and Diaz, 2016), such as how STPA can consider process hazards like pipe leaks, alarm problems, and how the process variables can

be considered (pressure, flow, composition, temperature, and others). Some questions still need to be solved like how to define system limits among thousands of variables and controllers. Future studies can be conducted on other process industry applications to identify workflows of multiple controllers and determine timing and sequencing of each control action, to reduce elapsed time between each step and introduce more sophistication in the process.

6 ACKNOWLEDGMENTS

The project is financed by *DynSoL AS and Research Council*, Norway, through research project number 283861 and performed at the *Department of Marine Technology, NTNU*. The authors of the paper wish to thank Professor Ingrid Bouwer Utne at the *Department of Marine Technology, NTNU*, for sharing her knowledge in system safety engineering and risk assessment; Børge Rokseth, Researcher at *Marine Technology Department, NTNU,* for sharing his experience of working with STPA on DP systems. We are thankful to Dr. A F M Kamrul Islam, Project Manager of DynSoL AS research project for his valuable support in HAZOP assessment.

7 REFERENCES

ABDULKHALEQ, A., LAMMERING, D., WAGNER, S., RODER, J., BALBIERER, N., RAMSAUER, L., RASTE, T. & BOEHMERT, H. 2017. A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles. *4th European Stamp Workshop 2016, Esw 2016,* 179**,** 41–51.

ABDULKHALEQ, A., WAGNER, S. & LEVESON, N. 2015. A comprehensive safety engineering approach for software-intensive systems based on STPA. *Proceedings of the 3rd European Stamp Workshop,* 128**,** 2–11.

ABRECHT, B. R. 2016. *Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System.* Massachusetts Institute of Technology.

AMES RESEARCH, C. 1973. *Failure mode, effects, and criticality analysis,* Moffett Field, Calif, National Aeronautics and Space Administration.

ANDOW, P. 1991. *Guidance on HAZOP procedures for computer-controlled plants*, Great Britain, Health and Safety Executive.

ASPINALL, P. HAZOPs, and human factors. INSTITUTION OF CHEMICAL ENGINEERS SYMPOSIUM SERIES, 2006. The institution of Chemical Engineers; 1999, 820.

BARLOW, R. E. & CHATTERJEE, P. 1973. Introduction to fault tree analysis. CALIFORNIA UNIV BERKELEY OPERATIONS RESEARCH CENTER.

CHATZIMICHAILIDOU, M. M., KARANIKAS, N. & PLIOUTSIAS, A. 2017. Application of STPA on Small Drone Operations: A Benchmarking Approach. *4th European Stamp Workshop 2016, Esw 2016,* 179**,** 13–22.

CHEN, J. Y., LU, Y., ZHANG, S. G. & TANG, P. 2015. STPA-based Hazard Analysis of a Complex UAV System in Take-off. *3rd International Conference on Transportation Information and Safety (Ictis 2015)***,** 774–779.

CRAWLEY, F. & TYLER, B. 2000. HAZOP: Guidelines to Best Practice for the Process and Chemical Industries

DONG, A. 2012. *Application of CAST and STPA to railroad safety in China.* Massachusetts Institute of Technology.

DROGOUL, F., ROELEN, A. & KINNERSLY, S. TOWARDS AN APPROACH TO BUILDING SAFETY INTO DESIGN. *Science,* 42.

DUNJÓ, J., FTHENAKIS, V., VÍLCHEZ, J. A. & ARNALDOS, J. 2010. Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials,* 173**,** 19–32.

EARGLE, L. A. & ESMAIL, A. 2012. Black beaches and bayous: the BP Deepwater Horizon oil spill disaster. University Press of America, Inc.

Failure Investigation Report – Liquefied Natural Gas (LNG) Peak Shaving Plant, Plymouth, Washington. Williams Partners Operating, LLC.

FLEMING, C. H. 2015. *Safety-driven early concept analysis and development.* Massachusetts Institute of Technology.

FLEMING, C., PLACKE, M. & LEVESON, N. 2013. Technical report: STPA analysis of NextGen interval management components: Ground interval management (GIM) and flight decn interval management (FIM). MIT.

GLOSSOP, M., LOANNIDES, A. & GOULD, J. 2000. *Review of hazard identification techniques*, Health & Safety Laboratory.

GOYAL, R. 1993. Hazops in industry. *Professional Safety,* 38**,** 34.

HOEL, F. 2012. Modeling Process Leaks Offshore Using STAMP and STPA. Institutt for produksjons-og kvalitetsteknikk.

HOEPFFNER, L. 1989. Analysis of the HAZOP study and comparison with similar safety analysis systems. *Gas Separation & Purification,* 3**,** 148–151.

HOPKINS, A. 2008. *Failure to learn: the BP Texas City refinery disaster*, CCH Australia Ltd.

HULIN, B. & TSCHACHTLI, R. Identifying software hazards with a modified CHAZOP. PESARO 2011 First Int. Conf. Performance, Saf. Robustness Complex Syst. Appl, 2011. 7–12.

ISHIMATSU, T., LEVESON, N., FLEMING, C., KATAHIRA, M., MIYAMOTO, Y. & NAKAO, H. Multiple controller contributions to hazards. 5th IAASS Conference, Versailles, France, 2011.

ISHIMATSU, T., LEVESON, N., THOMAS, J., KATAHIRA, M., MIYAMOTO, Y. & NAKAO, H. 2010. Modeling and hazard analysis using STPA.

KHAN, F. I. & ABBASI, S. A. 1999. Major accidents in process industries and an analysis of causes and consequences. *Journal of Loss Prevention in the Process Industries,* 12**,** 361–378.

KLETZ, T. 1995. Some incidents that have occurred, mainly in computer-controlled process plants. *Computer control and human error*.

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

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

LEVESON, N. G. A new approach to hazard analysis for complex systems. International Conference of the System Safety Society, 2003.

LEVESON, N. G. 2004. Model-based analysis of socio-technical risk.

LEVESON, N. G. 2011b. Applying systems thinking to analyze and learn from events. *Safety Science,* 49**,** 55–64.

LIAW, H. J. 2016. Lessons in process safety management learned in the Kaohsiung gas explosion accident in Taiwan. *Process Safety Progress,* 35**,** 228–232.

LUTZ, R. R. Analyzing software requirements errors in safety-critical, embedded systems. Requirements Engineering, 1993., Proceedings of IEEE International Symposium on, 1993. IEEE, 126–133.

MARAIS, K., DULAC, N. & LEVESON, N. Beyond normal accidents and high-reliability organizations: The need for an alternative approach to safety in complex systems. Engineering Systems Division Symposium, 2004. 1–16.

MAYER, G., ZUBIR, W. A., MING, L. A. & CHANG, R. Tele-Maintenance for Remote Online Diagnostic and Evaluation of Problems at Offshore Facilities, Sarawak. SPE Asia Pacific Oil and Gas Conference and Exhibition, 2003. Society of Petroleum Engineers.

MCDERMID, J. A., NICHOLSON, M., PUMFREY, D. J. & FENELON, P. Experience with the application of HAZOP to computer-based systems. Computer Assurance, 1995. COMPASS'95. Systems Integrity, Software Safety, and Process Security. Proceedings of the Tenth Annual Conference on, 1995. IEEE, 37–48.

NAKAO, H., KATAHIRA, M., MIYAMOTO, Y. & LEVESON, N. Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. Proc. of the 5: the IAASS Conference, 2011. Citeseer, 497–501.

NIMMO, I. 1994. Extend HAZOP to computer control systems. *Chemical engineering progress,* 90**,** 32–44.

OTHMAN, N. A., JABAR, J., MURAD, M. A. & KAMARUDIN, M. F. 2014. FACTORS INFLUENCING SAFETY MANAGEMENT SYSTEMS IN PETROCHEMICAL PROCESSING PLANTS. *The Journal of Technology Management and Technopreneurship (JTMT),* 2.

OUDDAI, R., CHABANE, H., BOUGHABA, A. & FRAH, M. 2012. The Skikda LNG accident: losses, lessons learned and safety climate assessment. *International Journal of Global Energy Issues,* 35**,** 518–533.

OWENS, B. D., HERRING, M. S., DULAC, N., LEVESON, N. G., INGHAM, M. D. & WEISS, K. A. Application of a safety-driven design methodology to an outer planet exploration mission. Aerospace Conference, 2008 IEEE, 2008. IEEE, 1–24.

PALTRINIERI, N., TUGNOLI, A. & COZZANI, V. 2015. Hazard identification for innovative LNG regasification technologies. *Reliability Engineering & System Safety,* 137**,** 18–28.

PASMAN, H. J. 2015. *Risk Analysis and Control for Industrial Processes-Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events*, Butterworth-Heinemann.

RODRIGUEZ, M. & DIAZ, I. 2016. A systematic and integral hazards analysis technique applied to the process industry. *Journal of Loss Prevention in the Process Industries,* 43**,** 721–729.

RASMUSSEN, J. & DUNCAN, K. 1987. *New technology and human error*, John Wiley & Sons.

RAUSAND, M. 2013. *Risk assessment: theory, methods, and applications*, John Wiley & Sons.

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

SAHEED, Z. S. & EGWAIKHIDE, C. 2012. Impact of social crises on economic development: Theoretical evidence from Nigeria. *American International Journal of Contemporary Research,* 2**,** 176–184.

STAMATIS, D. H. 2003. *Failure mode and effect analysis: FMEA from theory to execution*, ASQ Quality Press.

STONEBURNER, G., GOGUEN, A. Y. & FERINGA, A. 2002. Risk management guide for information technology systems.

SWANN, C. D. & PRESTON, M. 1995. Twenty-five years of HAZOPs. *J. Loss Prev. Process Ind.,* 8**,** 349–353.

THOMAS, J. 2013. *Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis.* Massachusetts Institute of Technology.

WUTC, P. 2016. Failure Investigation Report – Liquefied Natural Gas (LNG) Peak Shaving Plant, Plymouth, Washington. Williams Partners Operating, LLC.

YOUNG, W. & LEVESON, N. G. 2014. An integrated approach to safety and security based on systems theory. Communications of the ACM, 57, 31–35.

Table 2: HAZOP for LNG supply from storage tank of carrier ship to storage tank of FSRU

Parameter	Deviation	Causal factors	Consequences (system reaction)	Actions required
Flowrate	1.1 High	Ship pump malfunction, control valve malfunction, PLC failure, undefined procedure, boundary conditions, threshold value, Valve fully open due to debris, debris suddenly loosened	High level in tank, High flow over a period of time may cause flow induced vibration, may cause flow induced vibration, pipe rupture and leakage	Consider flow meter and high-level alarm if not previously identified, clarify design basis
	1.2 low	Ship pump malfunction, wrong rout, fouling of valves, density change, valve not fully open	Storage tank filling time too long	The conditions under which the flowline can be operated needs to be investigated to ascertain if resulting boundary conditions are valid
	1.3 No	Valve stuck, line blockage, pipe or vessel rupture, large leak, equipment failure, gas lock, pump failure, line blockage, PLC functions wrongly	Pump runaway, explosion, loss of production Explosion, loss of production, pump overheats, LNG loss via relief valves	Consider installation of low-level alarm on tank plus low-level trip to stop pump, regular inspection and patrolling of transfer line Install kickback on pump Check design of pump strainers Place controller for critical instruments
	1.4 Reverse	Valve failure	Pipe breaks, process upset	Additional measures to protect against operational failures
	1.5 Flow-induced vibration	High flow, siphon effect, emergency venting, incorrect operation, pump failure, pump reversed	Stress to the material may lead to fatigue and cracking and ultimately loss of piping.	There is an ongoing study, and it should be verified that the study incorporates the maximum speed that will be encountered
	1.6 Leakage through the line	Internal leakage in valves	Process upset	The risk of leak/leak size and the consequences on facility to be evaluated should be identified. The potential risk should be flagged and accepted by facility
Pressure	2.1 High	PCV failure, inadequate volume of vents, external fire, weather condition, changes in density, external fire	Fire, explosion, fluid loss, water hammer on site, rupture of pipe	Assess risk and redesign pressure protection system Adjust PSV set points, implement new shut down functions, improve reliability of shut down functions, improve operational procedure
	2.2 Low	Undetected leakage, restricted pump/compressor line, vessel drainage, imploding, fire condition, weather condition, vent valve open, sunction line plugged, cavitation, phase change of LNG	Fluid loss & explosion/fire risk	Adjust PSV set points, improve operational procedure

Parameter	Deviation	Causal factors	Consequences (system reaction)	Actions required
Temperature	3.1 high	Ambient condition, fire situation, defective control valve, internal fire, faulty instrumentation and control, cooling system fail, mechanical heating	LNG loss via relief valve	Improve reliability of thermal valves,
	3.2 Low	Ambient conditions, faulty instrumentation and control	Fluid loss & explosion/fire risk, risk of rupture	Improve reliability of instruments
Composition	4 Abnormal contamination	Bad LNG quality from ship, leaking isolation valves, incorrect operation of system, ingress of air, ingress of water, corrosion, gas entrainment	LNG inside tank polluted Corrosion or erosion inside pipe	Check design basis against operational experience
Concentration	5 Low	Impure raw material, leak in line, phase change, process control upset, gas entrainment	Performance of equipment gets affected, Impure product, Chances of severe working conditions	Check material quality
Level	6.1 high	Ship does not stop unloading (operator mistake or pump malfunction), outlet isolated or blocked, faulty level measurement, corrosion, pressure surge, Wrong level information (sensor problem), leakage on storage tank	Fluid leakage on PRV due to pressure increase	Install reliable level sensor Take protection for corrosion, blockage
	6.2 Low	Inlet flow stops, leak, control failure, faulty level measurement	Longer unloading operation, fire risk	Install reliable level sensor
Service failure	7	Electric power, water supply, telecommunications, PLCs/computers, HVAC, fire protection, steam	Abort of operation	Check for alternate electricity, water
Abnormal operation	8	Emergency shutdown, emergency operation, inspections of operating machines, guarding of machinery	Personal injury, risk of fire, financial loss	Improve operational procedure, engage qualified personnel for operation, arrange training to handle emergency
Maintenance/procedures	9	Drainage, purging, cleaning, access, rescue plan, pressure testing, work permit system, condition monitoring	Late or cancelled operation, equipment failure	Maintain proper maintenance log
Static	10	Insulated vessels, hot work, hot surface	Personal injury, risk of fire	Avoid hot work during operating, maintain proper work permit system
Spare equipment	11	Availability of spares, storage of spares, catalogue of spares	Interrupted operation	Establish standard spares supply system
Information	12	Confusing, inadequate, missing, misinterpreted, wrong information	Incorrect operation	Arrange good telecommunication system

Parameter	Deviation	Causal factors	Consequences (system reaction)	Actions required
Sequence	13	Operation too early, operation too late, operation left out, wrong action in operation	Financial loss, Risk of accident	Establish standard operational procedure
Global	14	Weather (temperature, humidity, flooding, winds, sandstorm), geological or seismic, human factor (labelling, instructions, training), fire and explosion	Risk of accident	Establish network to provide weather forecast Take preventive measures for fire and explosion

Table 3: High-level system hazards, safety constraints, process model variables and possible control actions in the process for each intermediate accidental event

High-level System hazards	High-level Safety constraint	Process model variables	Examples of control actions
H1: High pressure in system	Pressure in system should not exceed a defined limit Temperature in system should not exceed a defined limit Fire occurred nearby should not affect the system	High pressure in system High temperature in system	Activate pressure relief valve Extinguish fire Check insulation on pipeline Activate vent valve
H2: Low pressure in system	Pressure in system should not be below a defined limit	Low pressure in system Pump speed	Check pressure control valve Check vent valve Regulate pump speed as desired Check for leak in system Protect system against leak
H3: High temperature in system	Temperature should not exceed a defined limit Pressure in system should not exceed a defined limit Fire occurred nearby should not affect the system	High temperature in system High pressure in system	Activate thermal relief valve Protect the system from ambient condition Extinguish fire Check insulation on pipeline Check control valve
H4: Low temperature in system	Temperature in system should not be below a defined limit	Low temperature in system Low pressure in system	Check for leak in system Check pipeline insulation

High-level System hazards	High-level Safety constraint	Process model variables	Examples of control actions
H5: Liquid level exceeds the high limit of storage tank	Liquid level should not exceed a defined limit	Liquid level high	Stop pump Check pipe network for blockage
H6: High flowrate in pipe	Flowrate should not exceed a defined limit	High flowrate	Control flowrate Check pump functionality Check valve functionality Check pipe network for debris Define operational parameters clearly
H7: Low flowrate in pipe	Flowrate should not be below defined limit	Low flowrate	Control flowrate Check pump functionality Regulate pump speed as desired Check valve functionality Check pipe network for debris Check pipe network for leak
H8: Flow induces vibration in system	Flow should not induce vibration in system	Possibility of incorrect operation	Check operational parameters Check equipment for vibration
H9: Process control upset	Operation should be performed in proper operational boundary	Operational parameters	Define operational parameters properly Execute operation maintain proper operational boundary
H10: Phase change of product during operation	Phase change should not occur during operation	Pressure Temperature	Execute operation maintain proper operational boundary
H11: Lack of electric power supply during operation	Electricity should be available during operation	Availability of electricity	Provide alternate electricity when regular supply not available
H12: System affected by external waves	System should not be affected by external waves	Requirement for emergency action	Activate emergency relief valve Open ERC
H13: System gets affected by external wind	System should not be affected by external wind	Presence of leak in system	Open ERC
H14: System gets affected by dropped object	System should not be affected by dropped object	Possibility of dropped object	Open ERC Shutdown of operation
H15: Corrosion	Corrosion should not cause leak in pipeline	Possibility of corrosion	Check pipe network for corrosion Take protective measures against corrosion Check product quality
H16: Presence of debris in pipeline	There should not be any debris in pipeline	Possibility of debris in pipeline	Check LNG quality from carrier ship

High-level System hazards	High-level Safety constraint	Process model variables	Examples of control actions
			Check for debris/particles in pipeline
H17: Undesired composition of LNG	LNG composition should be same as defined in protocol	Undesired LNG composition Functionality of valve	Check LNG composition from carrier ship Check control valves Check other operational parameters
IE: Presence of leak in system	Leak from system should not hamper the operation Leak should not lead to fire or explosion	Presence of leak in system	Leak mitigation Prevent ignition Prevention of fire Explosion prevention Prepare for emergency rescue action Follow operator safety protocols

Table 4: Hazardous control actions

No	Control action/event	Control action not provided causes hazard	Control action provided when not required causes hazard	Control action provided too early causes hazard	Control action provided too late causes hazard	Control action stopped too soon or applied too long
1	Activate PRV	PRV valve is not activateed when pressure/temperature exceeds high limit	PRV activateed when pressure/temperature is within range	N/A	PRV/PSV is activateed too late after detection of high pressure/temperature	N/A
2	Mitigate fire	Fire protection system is not activated when there is fire	Fire protection system is activated when there is no fire	N/A	Fire protection system is activated too late when there is fire	Fire protection system gets off before fire is mitigated
3	Check insulation on pipeline	Pipeline insulation is not checked regularly, and insulation protection is not taken	N/A	N/A	N/A	N/A

No	Control action/event	Control action not provided causes hazard	Control action provided when not required causes hazard	Control action provided too early causes hazard	Control action provided too late causes hazard	Control action stopped too soon or applied too long
4	Check valves functionality	Regular maintenance check on valve is not done	N/A	N/A	N/A	N/A
5	Regulate pump speed as desired	Pump speed cannot be regulated as desired	N/A	N/A	N/A	N/A
6	Check for leak in system	Leakage in system is not checked	N/A	N/A	N/A	N/A
7	Protect system against leak	Leak protection is not taken	N/A	N/A	N/A	N/A
8	Protect the system from ambient condition	Protection of system form ambient condition not executed	N/A	N/A	Protection of system form ambient condition executed too late	N/A
9	Execute operation in proper operational boundary	Operational parameters not maintained properly	N/A	N/A	N/A	N/A
10	Provide alternate electricity when regular supply is not available	Alternate electricity not available in case of unavailability of regular supply	N/A	N/A	N/A	N/A
11	Control flowrate	Flow rate cannot be controlled when flow is not within range	N/A	N/A	Flow rate is controlled too late when flow is not within range	N/A
12	Check pump functionality	Regular maintenance check on equipment is not done	N/A	N/A	N/A	N/A

No	Control action/event	Control action not provided causes hazard	Control action provided when not required causes hazard	Control action provided too early causes hazard	Control action provided too late causes hazard	Control action stopped too soon or applied too long
13	STOP pump	Pump is not closed when liquid level is high	Pump is closed when liquid level is not high	N/A	Pump is closed too late when liquid level is high	N/A
14	Check pipe network for debris	Presence of debris not checked	N/A	N/A	Presence of debris checked too late	N/A
15	Activate ERV	ERV is not activateed when emergency action is required	ERV is activateed when emergency action is not required	N/A	ERV is activateed too late	N/A
16	Take precautions for corrosion	Corrosion prevention action was missing	N/A	N/A	Corrosion prevention action was too late	N/A
17	Check LNG composition	LNG composition was not maintained	N/A	N/A	N/A	N/A
18	Prevent ignition	Ignition prevention procedure was not followed	N/A	N/A	Ignition prevention procedure followed too late	N/A
19	Activate fire suppression system	Fire suppression system is not activated when fire is detected	Fire suppression system is activated when fire is not detected	N/A	Fire suppression system is activated too late	N/A
20	Take emergency rescue action	Emergency rescue action was not followed	N/A	N/A	Emergency rescue action was followed too late	N/A
21	Follow operator safety protocols	Operator safety procedure was not followed	N/A	N/A	N/A	N/A

Table 5:Causal factors and low level safety constraints for each hazardous control actions

Hazardous control actions	**Causal factors**	**Low level safety constraints**
Pressure relief valve is not activateed when pressure/temperature exceeds high limit	1. Pressure sensor failure 2. Pressure relief valve failure 3. Communication error 4. Auto-activation is turned off 5. Problem in decision-making arrangement 6. Electricity blackout 7. Operator is reluctant to take action due to high workload 8. Poor audibility/visibility of sensor 9. Operator is confused about the procedures to be followed	1.1 Sensors must be designed to operate for X years with no defect 1.2 Sensors must be tested every Y year 1.3 Sensors must be replaced every Z year 2 Valves should be tested every Y year 3 Good communication arrangement between control room operators and site operators 4 Mode of each system/component should be defined clearly 5.1 Operator should know in which mode each component is working 5.2 Operator should know which control actions will be performed by auto controllers and which will not 5.3 Operators should know the timeframe within which auto controllers need to activate and maximum time which should be allocated until controllers take action 6 Alternate energy source should be available 7 Operator's maximum working time should be following according to regulation 8 Audibility/Visibility of sensor should be checked before starting operation 9 Should be trained for operating each component and valve manually
Pressure relief valve is activateed when pressure is within range	1. Pressure sensor malfunction 2. Communication error	Mentioned earlier
Fire suppression system is not activated when fire is detected	1. Detector malfunction 2. Communication error (missing signal) 3. Operator is reluctant to take action due to high workload 4. Poor audibility of detector 5. Operator is confused about the procedures to be followed	Mentioned earlier
Fire suppression system is activated when there is no fire	1. Detector malfunction 2. Communication error	Mentioned earlier
Pipeline insulation is not checked regularly, and insulation protection is not taken	1. Job is not included in maintenance log 2. Operator is reluctant to perform the task 3. Lack of operator training 4. Lack of trainer in the organization 5. Insulated pipe is not provided during installation	1. Update maintenance log regularly 2. Follow standard working time of operator 3. Provide adequate training and trainer to operators 4. Provide good insulated pipe

Hazardous control actions	Causal factors	Low level safety constraints
Instrumentation's functionality check was not done regularly	1. Job is not included in maintenance log 2. Operator is reluctant to perform the task 3. Lack of operator training 4. Lack of trainer in the organization 5. Lack of reliability of equipment	1. Provide reliable instruments and valves 2. Others mentioned earlier
Pump speed cannot be regulated as desired	1. Pump malfunction 2. Electricity blackout 3. Operator is reluctant to take action due to high workload 4. Operator is confused about the procedures to be followed	1. Pump should be checked before operation whether working, should be checked for maintenance after regular interval
Leakage in system is not checked and precaution for leak protection is not taken	1. Leakage check is not included in maintenance log 2. Temperature or pressure exceeds the defined limit 3. System not protected from high wave, wind, dropped object	1. Include leakage check in maintenance log 2. Follow precaution to keep the temp and pressure within boundary 3. Follow precaution to avoid dropped object 4. Protect the system high wave, high wind or other accident
Protect the system from ambient condition not executed	1. Weather data is not available to operators due to network failure 2. ERC/ERV not activated on time	1. Provide updated weather forecast to operators 2. Check ERC/ERV for maintenance regularly
Operational parameter not maintained during operation	1. Parameters not defined clearly to operators 2. wrong sensor information 3. control valve dysfunction	1. Define parameters clearly with detailed scope, should be written and updated regularly 2. Provide reliable sensors and control valves, check for maintenance regularly
Flow rate cannot be controlled when flow is not within range	1. Flow regulator not working 2. Wrong sensor information 3. Wrong voting arrangement or logic control malfunction 4. Pump malfunction 5. Lack of operator efficiency	1. Provide reliable logic controller Other LLSCs mentioned earlier
Pump is not closed when liquid level is high	1. Level Sensor failure 2. Communication error 3. Auto-activation is turned off 4. Pump malfunction 5. Problem in decision-making arrangement 6. Electricity blackout 7. Operator is reluctant to take action due to high workload 8. Poor audibility/visibility of sensor 9. Operator is confused about the procedures to be followed	1. Pump should be checked before operation whether working, should be checked for maintenance after regular interval

Hazardous control actions	**Causal factors**	**Low level safety constraints**
Missing Debris/external particle check and prevention	1. Operator is reluctant to take action due to high workload 2. Pipe leaked, and pollution occurred 3. Debris/Particle check procedure not followed	1. Follow pollution prevention strategy
ERV not activateed when emergency action is required	1. Wrong voting arrangement 2. Communication error 3. ERV malfunction 4. Electricity blackout	1. Provide alternate electricity supply
Corrosion prevention action missing or too late	1. Operator is reluctant to take action due to high workload 2. Corrosion check procedure is missing	Pipe should be covered with insulator
LNG composition was not maintained	1. Product quality check is missing	1. Follow standard quality check procedure
Ignition prevention procedure was not followed	1. Ignition prevention strategy was not followed	1. Keep control of explosive material in the plant 2. Keep control of Friction, Impact, Static and Heat energy sources in the plant and take precaution accordingly
Alternate electricity is not provided in case of unavailability of regular supply	1. Connection problem of DC power supply 2. Insufficient DC power supply	1. Include connection check of DC power supply in maintenance log 2. Calculate DC power requirement for each valves, sensors and other required equipments
Emergency rescue action was not followed or followed too late	1. Late arrival of emergency rescue team 2. Improper training of crew about emergency rescue action 3. Emergency rescue equipment malfunction	1 Team should be trained to take quick action and should be equipped properly 2 Crew should be trained to take emergency control action 3 Rescue equipment should be checked for maintenance after regular interval
Operator safety protocols were not followed	1. OSP was not provided 2. Training was not enough 3. Operator error due to high workload	4 OSP should be provided in detail

Table 6: Comparison between HAZOP and STPA

Hazard category	Identified by HAZOP? Examples	Identified by STPA? Examples
Component error	Ship pump malfunction Sensor malfunction PRV/control valve/check valve dysfunction Logic control failure Vent valve dysfunction Low audibility/visibility of sensor Equipment failure	Ship pump malfunction Pressure or level sensor malfunction in functionality, audibility or visibility Detector failure Control equipment malfunction Emergency rescue equipment malfunction Fire suppression system malfunction
Organizational error	Unloading procedure mentioned in protocol was not followed Ignorance about operational boundary (Flow, Pressure, Temperature) Ignorance about operational condition (empty tank, pressure, temperature, level) Mismanaged work permit system Improper condition monitoring Improper inspection of operating machines Emergency operation Incorrect rescue plan Incorrect pressure testing Permission for hot work during operation Availability of spares	Alternate system is not available during maintenance due to lack of redundancy or planning Standard working time is not followed Lack of healthy working environment Lack of well documented operational procedure Insufficient planning before operation Lack of well-trained resource, Lack of training about equipment handling, emergency rescue action, corrosion check, leak check Lack of communication between interdisciplinary team Lack of satisfaction of workers about workplace, salary or provided facility Wrong decision making by managers in the operational procedure Update of maintenance log is not performed, Low reliability of equipment or instruments Insufficient redundancy of equipment Poor planning of operation, Lack of existence or implementation of accident prevention strategy (high wave, wind, ignition, dropped object) Lack of operators' safety procedures
Human error	Valve half closed/fully closed during operation Bad LNG composition, Debris in pipeline External Water/particles inside product Remaining pressure in line Operator gives the wrong command More than needed wax/scale inhibitor is injected Wrong operational procedure Wrong information about pressure, temp, level Inadequate or missing or wrong information	Operator not aware of operating condition or system condition or instrumentation malfunction or product quality Missing action of operator due to high workload or dissatisfaction about work Wrong action of operator Wrong operational procedure Late arrival of emergency rescue team Maintenance log is not updated regularly Poor insulation of pipe or product quality check
Software error	Valve half closed/fully closed during operation	Wrong voting arrangement Bug in software

Hazard category	**Identified by HAZOP? Examples**	**Identified by STPA? Examples**
		Intentional sabotage or hacking of software
System or design error	Electricity blackout Leakage on line Line blockage Wrong rout Pipe or vessel rupture Large leak Internal leakage in valves Overpressure/ overheating due to fire/PRV failure Insulation failure Liquid accumulation in line, Remaining pressure in line Unwanted shutdown of system Missing emergency rescue action, Flow induced vibration Local instrument missing Incorrect operation Sedimentation Inadequate volume of vents Cavitation Mechanical heating Ingress of air Ingress of water Corrosion Gas entrainment Phase change Process control upset Electric power supply Telecommunication	Electricity blackout, Communication error Leakage on line Overpressure/ overheating of equipment Insulation failure Missing emergency rescue action Poor or missing insulation of pipe System is not protected against high wave, wind or dropped object Logic control system malfunction Incorrect operation Inadequate volume of vents Phase change Process control upset Unavailable electric power supply
External events	External fire Weather condition	System gets affected by wind, wave or dropped object