Integrated Process Systems Hazard Analysis (IPSHA): A Resilience-Based Approach

Prerna Jain*, William J. Rogers, Hans J. Pasman and M. Sam Mannan

Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering

Texas A&M University, College Station, Texas-77843-3122, USA

*pjain77@tamu.edu, +1(979) 985-0773

The chemical process industry has witnessed increased process safety management challenges and changes in global public perceptions of risk. Hence, it is critical to prioritize safer operations of process systems through effective methods and techniques. One of the initial steps in process safety and risk management of any facility is hazard identification and analysis. Hazards analysis is applicable to a process facility throughout its life cycle, from the design stage to the decommissioning or abandonment phase. With the conventional process hazard analysis (PHA), such as What-if analysis, Hazard and Operability (HAZOP) study and others, there is a tendency to overlook the systems aspect. This leads to ignoring social and human factors, such as shift handover communication, downtime, operating and maintenance procedures, and more. Two types of factors: 1) technical (e.g., equipment malfunction, process parameter variation), and 2) social (e.g., regulations/policy, human and organizational factors) are important in analyzing hazards of a socio-technical process system as a whole. This need calls for the development of a holistic and integrated systems framework for hazard analysis. The application of a resilience engineering perspective is gradually being explored as an approach for modeling the dynamics of socio-technical aspects based on systems theory.

This paper presents a novel hazards analysis approach for incorporating both technical and social factors within a single analysis method- Integrated Process Systems Hazard Analysis (IPSHA). The IPSHA approach is based on resilience aspects, which are Early Detection, Error Tolerant Design, Plasticity, and Recoverability. This work establishes and presents worksheet based on resilience metrics for analysis of hazards within process systems. The paper concludes with a case study to illustrate the key concepts of this study and the integrated approach.

Keywords: Resilience, process safety, risk management, organization, human, system

Introduction

In recent years, it has been observed that the increasing development in technology and rising awareness amongst members of the public have led to process safety and risk management challenges. Incidents have continued to occur in the process industry due to various reasons, such as complex technology, energy saving in view of climate change, better process efficiency, a series of human and organizational changes - fatigue due to long hours, less competence and indifference, rapid job rotation, retirement, job insecurity, time pressure, bad maintenance, less inspection by government, *etc.* in spite of the advanced risk management methodologies implemented (Jain, Pasman, Waldram, Rogers, & Mannan, 2016). Process hazards are mainly observed to be responsible for consequences such as fire, explosion, or toxic release. Due to this observation, often a holistic analysis of the whole system to understand the anatomy of an incident leading to a major catastrophe is missed in the current hazard and risk analysis techniques (Rathnayaka, Khan, & Amyotte, 2011b). Some of the remarkable incidents in process industry, such as the Bhopal tragedy (Eckerman, 2005; F. I. Khan & Abbasi, 1999; Willey, Hendershot, & Berger, 2007), the Piper Alpha (Flin, 2001; Flin, Mearns, Gordon, & Fleming, 1996; Pate-Cornell, 1993), the Flixborough disaster (Kletz, 2001; Tauseef, Abbasi, & Abbasi, 2011), BP Texas city (Holmstrom et al., 2006; Le Coze, 2008), the West fertilizer explosion (Pittman et al., 2014), and the Tianjin explosion, are examples of sociotechnical systems failures. According to Rathnayka et al., one of the leading causes of process system failures is increased complexity of system elements (people, equipment, procedures, software, and hardware) and their interactions (Rathnayaka, Khan, & Amyotte, 2011a).

Essential initial steps in process safety and risk management of any facility are hazard identification and hazard analysis. A large volume of work can be found in the literature on different hazard identification and analysis techniques and advanced methodologies, as summarized in section 2.1. (Dunjó, Fthenakis, Vílchez, & Arnaldos, 2010; F. Khan, Rathnayaka, & Ahmed, 2015). However, these methods have been considered inadequate in identifying and analyzing the majority of hazards involved in most incidents. This is because these techniques ignored the contribution of human, procedures or organizational elements that affected the analysis results (Suokas, 1988; Suokas & Rouhiainen, 1989). Most traditional methods use a linear approach and a single cause-consequence pair (Bruce K. Vaughen, 2016). These methods are not complete and lack a comprehensive assessment approach for the system. According to Zhao *et al.*, humans work with technology, social structures, and environment, which can be designated complex systems. In case of an accident system independencies must be addressed, and to inhibit such accidents the complete sociotechnical system must be evaluated (Zhao, McCoy, Kleiner, Smith-Jackson, & Liu, 2015). Therefore, a socio-technical systems perspective covering proper and adequate hazard identification including both technical (*e.g.*, equipment malfunction, process parameter variation, and social (*e.g.*, regulations/policy, human, and organizational) factors in the process plant system are paramount in development of preventive measures for catastrophic incidents. The socio-technical systems theory has been developed and explored by numerous researchers in the past (Katz & Kahn, 1978; Kleiner, 2006; Pasmore & Sherwood, 1978; Rasmussen, 1997). It is characterized as a complex organization with interaction among its elements of human and technology/equipment.

In the present work, a systems-based approach is further developed by including resilience engineering aspects. This results in creation of a holistic view of the hazard identification and analysis process called IPSHA (Integrated Process Systems Hazard Analysis), which can be applied to different modes and subsystems of the process system. To show the usefulness of the proposed approach, IPSHA is applied to the hazard identification and analysis of the liquefied natural gas (LNG) process system.

Background and motivation

This section presents the review of selected, existing hazard identification and analysis techniques gathered from the literature. Further, it presents a brief review of system and process hazard analysis.

Review of existing hazards identification and analysis techniques

There are a number of hazard evaluation techniques used by the process industry as a systematic method to identify influences or causes that may result in incidents or process upsets. (Gressel & Gideon, 1991) presented a review of the eight most commonly used hazard analysis techniques. These included checklists, what-if analysis, safety reviews, preliminary hazard analysis (PHA), failure mode and effect analysis (FMEA), fault tree analysis (FTA), event tree analysis (ETA), and hazard and operability study (HAZOP).

It was found that earlier researchers focused mainly on the conventional methods of hazard analysis (Hoepffner, 1989; Knowlton, 1987; Lawley, 1974). Later, researchers extended the work to include new types of deviations or automating the methods or exploring development of expert systems (F. I. Khan & Abbasi, 1997a, 1997b, 2000; Venkatasubramanian, Zhao, & Viswanathan, 2000; Wang, Gao, & Wang, 2012). Considering the batch processes as more critical, some authors focused their work in this area to identify and analyze hazards by developing advanced methods (Palmer & Chung, 2008; Srinivasan & Venkatasubramanian, 1996, 1998a, 1998b; Viswanathan et al., 1999). Also, researchers established hybrid approaches by combining HAZOP with dynamic simulation. (Viswanathan, Shah, & Venkatasubramanian, 2000). Furthermore, a comprehensive function based, systems framework approach called Blendid HAZID including system components as plant components, procedural aspects, and people was introduced (Cameron, Hangos, Lakner, Nemeth, & Seligmann, 2007; Cameron, Seligmann, Hangos, Németh, & Lakner, 2008; Seligmann et al., 2010).

It can be concluded that a considerable amount of work has been conducted through exploring and applying various methods, such as knowledge bases, combined with process models, such as petri nets, signed digraphs, and dynamic simulation, with focus on improving and semi-automating hazard identification. Nevertheless more research focused on systems thinking is needed for more effective hazard identification and loss prevention control. Of the various methodologies to identify and analyze hazards, specific consideration has been given to HAZOP. The HAZOP methodology is relatively convenient to implement and has been used by the risk assessors in process industry for very long time (Cagno, Caron, & Mancini, 2002).

Systems hazard analysis vs process hazard analysis

Process Hazard Analysis (PHA) is a methodical identification, assessment, and documentation of potential process hazards and incident scenarios related to a process plant. It is the most commonly used and easy to implement method used by process industry. It can be performed by using various techniques such as HAZOP, What-if analysis, safety review, and more.

It has been determined that numerous incidents in the process industry including the chemical, petrochemical, and offshore oil and gas platforms were not caused by a single reason or an independent failure. They were results of breakdown of various system components, such as organizational behavior, human errors, or procedural elements (Kariuki & Löwe, 2007; Kennedy & Kirwan, 1998; Raman, Gargett, & Warner, 1991; Rasmussen, 1997). Hence, it is critical to understand and analyze the human, procedures, and other social factors along with the technical factors like process parameters. It has been observed that PHA has a limitation where it lacks social and organization factors associated with the operations in a single approach (Schurman & Fleger, 1994).

Various research works have been carried out in field of system safety. The concept of safety culture and its relation to the system property was explained. (Reiman & Rollenhagen, 2014). Researchers have proposed different accident models demonstrating the influence of human, organizational, and managerial factors (Leveson, 2004; Reason, 1990; Svenson, 1991). Inspired by the smoothness of American aircraft carrier operations with emphasis on tracking and monitoring small failures, less oversimplification, sensitivity towards operations, ensuring resilience capabilities, and taking benefit of shifting locations of expertise, several researchers have proposed the HRO or High Reliability Organization concept. Weick & Sutcliffe, 2011 described the concept in extension and explained the (HRO) Principle of "Preoccupation with Failure", which focuses on several small errors that can lead to a bigger disaster. Hence by targeting smaller errors a catastrophic incident could be prevented (Weick & Sutcliffe, 2011).

As defined by Stephans, "System safety analysis is the formal analysis of a system and interrelationships among its various parts (including plant and hardware, policies and procedures, and personnel) to determine real and potential hazards within the system and suggest ways to reduce and control those hazards" (Stephans, 2012). Unlike PHA, systems hazard analysis (SHA) focuses on the complex combinations of subcomponents acting together. Macroergonomics is one of the proposed top-down approach for systems hazard analysis of a socio-technical system (Kleiner, 2006; Trist & Bamforth, 1951). The sociotechnical hierarchical structure has also been considered by (Rasmussen, 1997) and (Leveson, 2004) as a basis for analyzing holistic risk control of systems, while the organizational aspect has been emphasized in the resilience engineering initiative (Hollnagel, Woods, & Leveson, 2007).

IPSHA: a resilience-based approach

As described in previous sections, the majority of incidents in the process industry are a result of human, organizational, management, mechanical, and operational failures (Galán, Mosleh, & Izquierdo, 2007; Giardina & Morale, 2015). Current methods for hazard identification and analysis have focused on process hazards or researchers have explored isolated methods for human error analysis. Further, most methods lack the anticipation element and also the full anatomy of incident – initiation, propagation, and termination. The key methods used today in the industry follow a univariate analysis and are limited in their approach to consider multiple factors, complex interactions among system components and their relationships (Giardina & Morale, 2015). The hazard analysis method for a complex socio-technical system such as a process plant should have the following characteristics: consideration of all system components (processes, human operations, equipment, instruments, control systems, *etc.*), all plausible deviations, a multi-disciplinary team, and proper documentation. IPSHA is a novel hazards analysis approach based on resilience engineering concepts that incorporate both technical and social factors within a single analysis method. It has been found that HAZOP is the most widely used PHA method. Therefore, HAZOP is selected as the base methodology for IPSHA but embedded in resilience thinking. This means that the resilience concept in its totality should leave fewer overlooked deficiencies and make up for ones still remaining. The IPSHA methodology for hazard analysis includes the following features: applicable to the life cycle of the process system, dynamic in nature, emphasizes on social factors, such as organizational behavior and management systems.

Several authors have developed methods based on monitoring and analysis of trends or variations in parameters (Cheung & Stephanopoulos, 1990; Janusz & Venkatasubramanian, 1991; Rengaswamy & Venkatasubramanian, 1995). However, these parameters have been primarily limited to the process. The IPSHA methodology is based on parameters and guidewords developed based on resilience metrics from four aspects. This follows the well-established HAZOP technique and covers technical as well as social aspects of the process system. Therefore, the IPSHA methodology provides the following benefits:

- Analyzes both internal and external disruptions
- Considers static and dynamic states covering various modes

Process system

A process system is a chemical processing system, which uses some inputs such as raw materials, utilities, and energy to process them into manufactured products. This process system consists of various sub-systems such as equipment, operators, procedures, and a management system. There exist various levels, layers, and components that interact with each other following a certain set of requirements.

Process system resilience

Hollnagel et al. (Hollnagel, Nemeth, & Dekker, 2008) identified and developed four cornerstones of resilience engineering that are *anticipation*, *monitoring*, *response*, and *learning*. Based on these four qualities of a resilient system, we identify four aspects of the process resilience analysis framework. These are *early detection*; *error tolerant design* including inherently safer design*;* *plasticity*, also characterized as resistive flexibility, and *recoverability*, as shown in Figure 7 (Jain et al., 2016).

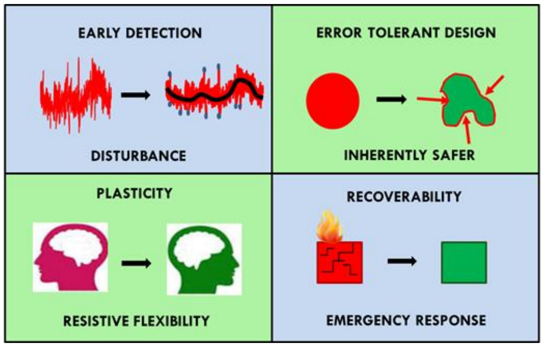

Figure 1: Process system resilience aspects (Jain et al., 2016)

Early detection refers to the recognition of systems' 'weak' signals that could be precursors of one or more undesired event. Error tolerant design presents the inherently safer features of a system and process such that undesired, and perhaps even unknown, external influences will not cause the system to fail in any significant way. The process still functions well (but perhaps at reduced efficiency). Recoverability presents how quickly the system can recover back to the normal state of operations. Finally, plasticity refers to the seamless transition from a normal state to an upset state and how the organization and people would behave or be affected. Resilience metrics (See Appendix A) have been developed with respect to each of the aspects. We use the resilience definition given by Jackson for process system resilience. It is defined as the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions (Jackson, 2009). Process system resilience is applied through 3 different phases of avoidance, survival, and recovery (Jackson, 2009; Jain et al., 2016).

Bi-layered approach

The system approach refers to both the vertical layers of Engineering, Safety & Security, Procurement, Construction, and Contracting activity and also the horizontal layers of an operational plant/facility. This paper addresses mainly the latter. The IPSHA methodology proposes a bi-layered approach that takes into account the two distinct layers, as shown in Figure 2:

Corporate systems hazard analysis

This is the first layer called the corporate system, and it can be further broken down into three rational sub-systems for analysis: process safety culture and leadership; operational discipline, and process safety systems. It has been observed that deficiencies in these sub-systems lead to weaknesses of the whole system potentially causing disastrous consequences. An important or critical example of a hazard due to organizational factors is lack of proper synthesis of performance with safety given priority that can result in reduced vigilance to maintain standards of risk and a degradation of organizational resilience. Lee *et al.* provided benefits of resilience metrics as progress towards being more resilient; need for leading indicators for resilience; improvements linking competitiveness and organizational resilience and demonstration of a business case for resilience (Lee, Vargo, & Seville, 2013). The analysis for this first layer is 'work in progress' and hence not presented in this paper.

Plant systems hazard analysis

This is the second layer called the plant system and is further broken down into the three rational sub-systems for analysis (human, procedures, and plant equipment). This supports capture of deviations arising from each of the sub-systems and also their interactions. A detailed method for this layer is presented in this paper.

Human: humans or the operators in the plant form an important sub-system as they recognize actions to be taken based on standard operating procedures and information from the control systems panel. (Taylor, 2013) raised concern related to the minimal use of human error analysis in the petroleum, petrochemical, and chemical industries. An error analysis method was proposed to identify error causes, which are helpful in defining preventive measures incorporating human reliability techniques into the design. Human error is attributed to be responsible, directly or indirectly, for 50-90% of the operational risk (Baybutt, 2002; Dunjó et al., 2010).

Procedures: standard operating and maintenance procedures play a crucial role in process safety (Aelion & Powers, 1993). These provide information to operators to perform various tasks sequentially in a complex plant setting. Researchers have mentioned that hazards analysis application to procedures would help predict potential deviations, failures in procedures, and human errors that could help prevent catastrophic incidents (Raman et al., 1991).

Process/Plant equipment: process hazards have been well-covered by the traditional HAZOP guidewords. Regarding plant equipment based on the IPSHA approach, as attributes of a socio-technical system, reliability and maintainability of plant equipment are essential for high organizational resilience, but each is highly influenced, both directly and indirectly, by organizational factors. Design decisions involving these attributes greatly affect system life–cycle costs (direct and indirect) including costs of components, costs of failure events, and costs of maintenance. The true probability of failure on demand of a system component, which is not currently recognized by the majority of industry, is a sum of three contributions due to 1) random failure of a component, 2) failure due to component offline for testing, maintenance or replacement, and 3) excessive supply and administrative delays that increase MTTR (mean time to repair) due to organizational factors. Unavailability on Demand, QOD, is more realistic than PFD in capturing the overall failure uncertainty and component failure probability due to the sum of:

- Component random failure, PFD
- Component test and maintenance, MTTR, meantime to repair
- Organizational delays and supply delays: SAD, supply and administration delays

It is significant to note that organizational factors and associated hazards, enter both directly with SAD and indirectly with quality of training/retraining for testing and maintenance, quality and time of testing and maintenance, quality and time of maintenance and replacement. Furthermore, an important point to note is that QOD is a component resilience expression, because it includes the three parts of the overall probability of component failure and it includes restoration of a component that has been tested, maintained, or replaced following failure or detection of failure.

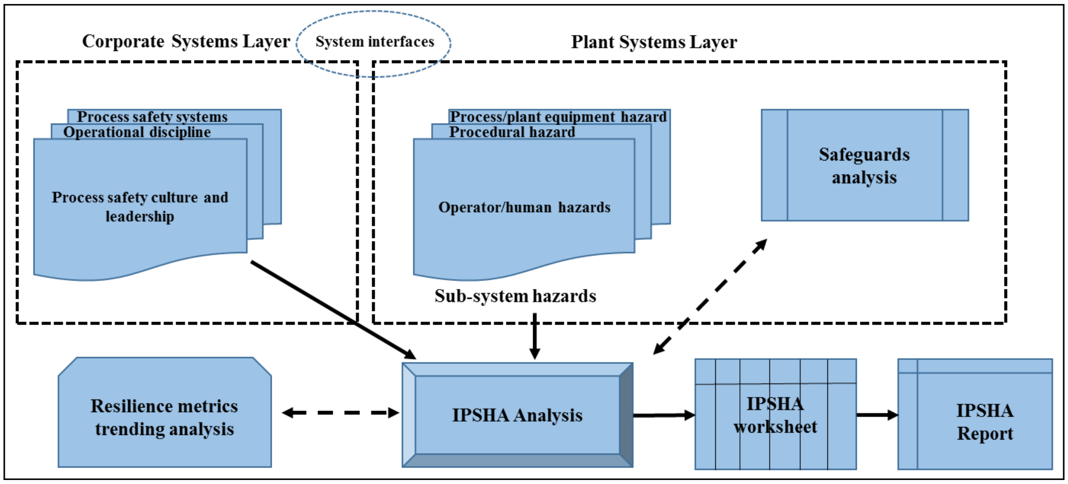

Figure 2: IPSHA: bi-layered approach

Multi-mode approach

The IPSHA approach is developed such that it can be applied to various modes in a process system. These modes are design, normal operations, and transient operations.

Design: Traditional HAZOPs are primarily conducted on the design and its verification in e.g., the commissioning stage. Hence, there is no doubt it is paramount for safety. However, human and procedural elements of the process system are often missed during the conventional methods, as well as to a lesser extent technical ones. Recently, there has been consideration given to this aspect (Chudleigh & Clare, 1993). Hence, IPSHA includes this as one of its modes for analysis.

Normal operations: This mode is the one that has been studied or analyzed well over the years. The IPSHA approach would follow the conventional HAZOP process for this mode.

Transient operations: A process plant is never in a single mode of operation and operates in different modes. Changing from one mode to another is called transition. Start-up, shutdown, catalyst changing and regeneration are some of the common examples of transient operations (Cagno et al., 2002; S.W. Ostrowski, 2008; Sundarraman & Srinivasan, 2003). It has been found in the literature that these operations are rare and involve high human intervention (S.W. Ostrowski, 2008). A large number of incidents have been reported to occur during transition operations (Nimmo, 1993; Sundarraman & Srinivasan, 2003) (S.W. Ostrowski, 2008). However, less attention has been paid to these operations. Therefore, it is critical to consider such operations in the IPSHA methodology.

Methodology

The IPSHA methodology has the following steps as part of the hazard identification and analysis:

Team formation

The IPSHA HAZOP team composition and experience requirements are similar to those for a traditional HAZOP with the following additional requirements or exceptions or features for design and transient operations modes:

- ***Design:*** design engineer who designs the function of the system; engineer who designs the human-machine interface (HMI); human factor engineer who determines the procedural elements, and an experienced representative from the operators group of a similar plant.
- ***Transient operations:*** an experienced operations representative with a sound knowledge of transient operations, their critical nature, field operations and controls through HMI; and a process design and technology expert with specific knowledge of the equipment and the process under review (S.W. Ostrowski, 2008).

Charter preparation

The IPSHA leadership team must prepare and issue a charter. The charter should define the responsibilities, tasks, and objectives of the team. It should also include the unit/operation selection, process boundaries, and any special objectives.

Data and documents collection

The IPSHA team should collect the following information:

- Material Safety Data Sheet (MSDS) of materials,
- Process design basis, and equipment design basis (including arrangement drawings, piping and instrument diagrams, plot plan, instrument logic diagrams, electrical diagrams),
- Operating and maintenance procedures
- Standard operating conditions (safe operating limits)
- Management of change documents (since prior PHA)
- Learning from incident and near miss reports (since prior PHA)
- Prior PHAs/IPSHAs (within the same boundaries)
- PHAs from similar processes, if applicable

The IPSHA team should review the documents and information for the system to be studied and ensure that it is sufficiently accurate for conducting the analysis. Any minor errors should be corrected. If there are serious deficiencies, the IPSHA team must stop work, report the problem to the IPSHA team leadership, and request that the information be updated. The IPSHA team, if during the course of conducting the analysis, determines any inconsistency with the plant's designation of safety critical components; equipment or procedures, must document that finding as a recommendation.

Sub-systems procedural review

The sub-systems procedural review should be carried out in a similar way as a regular HAZOP. The IPSHA worksheet is included in Table 2 to include the three modes (design, normal operations, and transient operations) and the three sub-systems (human, procedures, and plant equipment). Tables 2 and 3 list the selected guidewords for operator/human and the procedures sub-systems based on resilience aspects and metrics (See Appendix A). Guidewords or process/plant equipment are not presented here as these are similar to the conventional HAZOP.

Table 1: IPSHA worksheet

Project/Plant:													**Page: of**
Rev. no:													**Date:**
HAZOP team members:													
System description:													
Mode:													
Node (P&ID):													
Subsystem: Process/Plant equipment						**Subsystem intention**							
					Risk without any safeguards				**Risk with safeguards**				
Parameter	**Guideword**	**Deviation**	**Cause**	**Consequence**	**Severity (S)**	**Likelihood (L)**	**Risk (R)**	**Safeguards**	**S**	**L**	**R**	**Recommendations**	**Responsible entity**
Subsystem: Operator/human						**Subsystem intention**							
					Risk without any safeguards			**Risk with safeguards**					
Parameter	**Guideword**	**Deviation**	**Cause**	**Consequence**	**Severity (S)**	**Likelihood (L)**	**Risk (R)**	**Safeguards**	**S**	**L**	**R**	**Recommendations**	**Responsible entity**
Subsystem: Procedure						**Subsystem intention**							
					Risk without any safeguards			**Risk with safeguards**					
Parameter	**Guideword**	**Deviation**	**Cause**	**Consequence**	**Severity (S)**	**Likelihood (L)**	**Risk (R)**	**Safeguards**	**S**	**L**	**R**	**Recommendations**	**Responsible entity**

Table 2: Operator/human: suggested guidewords (Crowl, 2007; Jain et al., 2016; Schurman & Fleger, 1994)

Operator/Human: suggested guidewords			
Resilience aspect	**Resilience metric**	**Parameter**	**Guideword**
Plasticity	P9	Operator	Missing
Plasticity	P9	Action	Missing
			Mistimed
Plasticity	P4	Procedure	Mistimed
Plasticity	P3	Training	Missing
Plasticity	P9	Supervision	
Early Detection	ED1	Alarm	Skipped
Plasticity	P11	Detail	More
			Less
			Other than
Plasticity	P11	Communication	Shift changeover, Who should know (verbal/written)

Table 3: Procedure: suggested guidewords (Crowl, 2007; Jain et al., 2016; Raman et al., 1991)

Procedure: suggested guidewords				
Resilience aspect	**Resilience metric**	**Operations**	**Parameter**	**Guideword**
Plasticity	P5	Permit to work	Isolation (covering adequacy, type and location of isolations)	None
				Inadequate
				Wrong
			Tagging (valves, electrical, fire and gas, panels, utility systems)	None
				Inadequate
			Safety Equipment (extinguishers, fire blankets, cover drains, safety watch)	Not specified
				Inadequate for location
			Special Instructions (list of blinds, tag list, ESD locations, specific emergency instructions)	None
				Inadequate
			Maintenance Procedures	Not made available
				Inadequate
Plasticity	P4	Maintenance preparation	Process isolation	Inadequate
				Wrong location
				Wrong type
			Electrical isolation	Inadequate
				Location
			Mechanical isolation	Inadequate
				Wrong type
				Not to line/equipment specification
				Wrong location
			Instrument	Wrong location
				No back-up

				Interlock (trip) disconnected
			Depressurizing	Wrong location
				Too rapid
				Inappropriate
				None
				Inadequate
			Gas testing	None
				Inadequate
				Wrong location
			Purging	None
				Inadequate
				Wrong location
				Wrong medium
				Inadequate
				Shift changeover
				Crew changeover
Plasticity	P4	Maintenance	Maintenance Procedures	Unavailable to crew
				Inadequate
Early Detection	ED3		Inspections	None
				Incomplete
Recoverability	R1		Special Instructions (list of blinds, tag list, ESD locations, specific emergency instructions)	Process emergency
Plasticity	P11		Communication	Who should know (verbal/written)?
				Shift changeover
				Crew changeover
Plasticity	P7		Spares	Wrong Specification
Plasticity	P8		Reassembly (misalignment, wrong installation, temporary blinds not removed)	Incorrect
Plasticity	P8	Handback and restart	Isolation (relief valve, blowdown, temporary blind)	Not checked
			Tags	Not removed
			Logic (trips)	Not restored
			Pressure testing	None
				Inadequate
				Wrong
			Electrical connection	Premature
				Wrong
			Housekeeping (blocked drains, foreign objects, work area)	None
				Inadequate

Documentation of findings

While documenting the findings, the IPSHA team should address or reference the specific findings in the hazard analysis worksheet and use precise wording. The accountability for each finding or recommendation should be assigned to an individual.

Recommendations

After hazard analysis, following key points should be followed while making recommendations:

- recommendations must be made to provide additional safeguards where appropriate,
- clear connection with the process/human/procedure hazard,
- related to degree of risk
- consider the integrity and adequacy of safeguards such as independence, dependability, auditability, integrity

The IPSHA team should ensure that the findings, including the actions taken, are communicated to all employees whose work assignments are in the facility/system or who are affected by the recommendations or actions. Also, the results should be communicated to the emergency response (ER) team so that the ER team has the information needed to develop effective responses.

Closure of recommendations and corrective actions

The management should review the recommendations from the IPSHA study. The response from management must be documented to each recommendation, either accepting it as is, accepting it as modified, or rejecting it. A completion date should be assigned to each accepted/modified recommendation. An electronic system should be followed to track the recommendations. Corporate systems hazard analysis will be used to ensure corrective actions are taken and recommendations are closed timely. Following are the resilience metrics that are relevant for the corporate systems hazard analysis: ED_5, ED_6, ED_7, ETD_1, P_1, P_2, P_7, P_{12}, R_2 (See Appendix A).

Case study: a liquefied natural gas (LNG) facility

A typical LNG process system consists of the following process sections: gas production, pipeline transmission, liquefaction plant, shipping, regasification, and send-out (Huang, Chiu, & Elliot, 2007). The LNG storage tanks are common to all the LNG facilities, such as import/export terminals and the peakshaving facilities. Therefore, a LNG storage tank area is selected for the IPSHA analysis.

Natural gas is composed primarily of methane and contains minor amounts of ethane, propane, butane, nitrogen, and carbon dioxide. The major hazard associated with LNG is due to its cryogenic temperature, flammability (flammability range in air is between 5% and 15% by volume), and vapor dispersion properties. Figure 3 represents the simplified piping and instrumentation diagram for the LNG storage tank, which is common to a majority of LNG plants. The LNG storage tank used as the case study in this study is a double containment type. The transient operations mode is considered as an example in which tank start-up is studied and demonstrated.

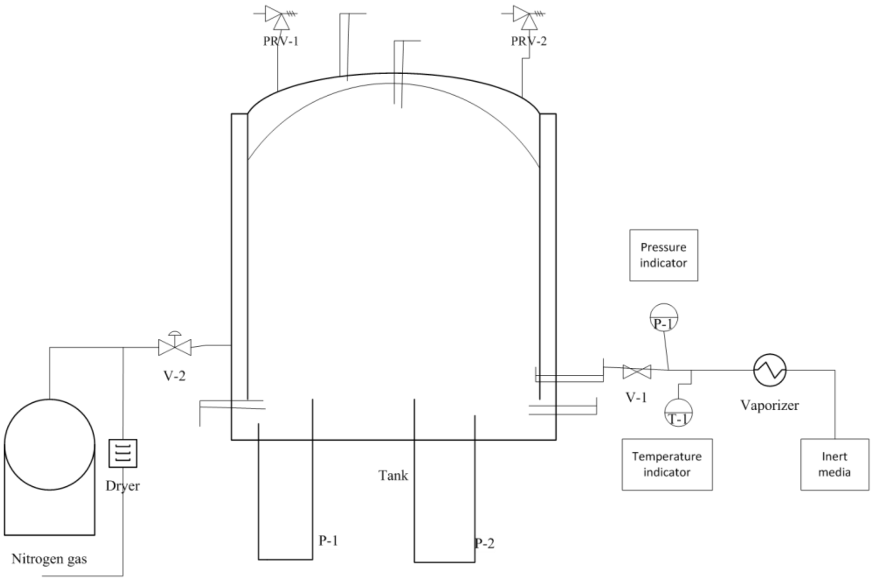

Figure 3: LNG storage tank P&ID

Based on the IPSHA methodology, a team is formed of members with knowledge about the tank start-up operations. The charter is prepared defining the scope of the study to the mentioned operations for this example. Information for each hazardous substance, in this case LNG stored, handled, and processed onsite is collected. The information is expected to include similar information required under 29 CFR 1910.119(d), such as physical and chemical properties, combustibility, flammability, and explosivity, toxicity, reactivity, and corrosivity. In addition, the vessels and piping containing these materials and associated process conditions are identified on drawings, such as PFDs, P&IDs, and plot plans. Furthermore, any near-miss or incidents reports also are gathered. As the next step, a sub-system procedural review is carried out using the sample guidewords and worksheet provided in Tables 1, 2, and 3. The case study results are presented in Table 4.

Table 4: IPSHA worksheet for plant systems layer analysis – LNG storage tank

Project/Plant:	XYZ											**Page:**	1 of 1
Rev. no:	0											**Date:**	28-Dec-16
HAZOP team members:	A, B, C, D & E												
System description:	LNG storage tank (start-up)												
Mode:	Transient operations												
Node (P&ID):	101												
Subsystem: Procedure	Start-up procedure			**Subsystem intention**		To ensure a safe and effective commissioning and transition to operations.							
					Risk without any safeguards				**Risk with safeguards**				
Parameter	**Guideword**	**Deviation**	**Cause**	**Consequences**	**S**	**L**	**R**	**Safeguards**	**S**	**L**	**R**	**Recommendations**	**Responsible entity**
Piping & equipment clean-up inspection	Incomplete	Incomplete piping/equipment clean-up	Specific clean-up procedure not followed	Damage of in-line equipment (pumps, valves) resulting in total failure	S2	L2	R2	Low point drains; end caps on piping	S3	L1	R2	Ensure proper cleaning procedures are followed, foreign particles are removed during installation	Commissioning & Construction engineer
Drying-out	Improper	Improper drying out	Poor/hurried planning and preparation	Water/water vapor can freeze in valves/pumps/low points in the piping; damage to valve seats; delay in start-up schedule; increased costs	S3	L2	R3	Accurate & detailed procedures; recordkeeping	S2	L1	R1	not required	_
Purging	Wrong medium	Wrong medium in purging	Lack of knowledge	Freezing of purge gas under cryogenic temperatures	S3	L1	R2	no safeguards	S3	L1	R2	Compatibility check of the purge gas (temperature & dryness)	Process engineer
Cooling down	Inadequate	Inadequate cooling down	Lack of cool down criteria analysis	Piping stress	S3	L2	R3	no safeguards	S3	L2	R3	Cool down large bore LNG piping using cryogenic vapor flow	Commissioning engineer
Subsystem: Process/Plant equipment	Storage tank			**Subsystem intention**		To store the cryogenic LNG liquid safely.							
					Risk without any safeguards				**Risk with safeguards**				
Parameter	**Guideword**	**Deviation**	**Cause**	**Consequences**	**S**	**L**	**R**	**Safeguards**	**S**	**L**	**R**	**Recommendations**	**Responsible entity**
Flow	High	High flow to tank	Operator inadvertently starts normal & spare pump	Overfilling	S4	L1	R3	High level alarm; pressure indication	S3	L1	R2	Provide interlock to avoid dual pump operation	I&C engineer
Subsystem: Operator/human	Field/control room operator			**Subsystem intention**		To follow the procedure and communicate effectively.							
					Risk without any safeguards				**Risk with safeguards**				
Parameter	**Guideword**	**Deviation**	**Cause**	**Consequences**	**S**	**L**	**R**	**Safeguards**	**S**	**L**	**R**	**Recommendations**	**Responsible entity**
Communication	Skipped/missed	Skipped/missed communication between field/CR operator	Procedures not followed; faulty communication equipment	Problems in cleaning-up or purging	S3	L2	R3	no safeguards	S3	L2	R3	Establish & follow communication protocol; ensure checklist, documentation is completed	Operations & Commissioning team

Conclusions

A review of current hazard identification and analysis methods was presented. It is observed that existing methods do not follow an integrated systems approach, and hence a new resilience-based IPSHA method has been proposed. This method follows the resilience metrics to develop guidewords for hazard identification and analysis. The approach is an integration of two layers – corporate systems (process safety culture and leadership; operational discipline, and process safety systems) and plant systems (process/plant equipment, operator/human and procedures). A significant feature of IPSHA methodology is that it covers three different modes of analysis – design, normal operations, and transient operations to be applied throughout the life cycle of a facility. In the IPSHA methodology, the hazard identification and analysis is based on four resilience aspects of early detection, error tolerant design, recoverability, and plasticity, and hence it considers both the technical and social factors in the analysis. Further, it is suggested to implement the IPSHA approach throughout the lifecycle of a project. The life cycle approach allows for the identification of issues early enough in the design phase to incorporate design changes and mitigate hazards more economically, and, at the same time, allows for the review to still be valid through detailed design. Continuing the review throughout detailed design, construction, commissioning, and throughout operation during the life-cycle of the facility ensures that the original siting analysis conducted is still valid for the life of the facility, and that the facility is constructed, tested, and operated in a manner consistent with the original siting analysis.

The IPSHA methodology is applied to a LNG case study, which provides a small example of a comprehensive and systematic method to identify and analyze hazards. It illustrates that a resilience-based approach supports reduction of uncertainty in reducing the impact of unknown scenarios by consistently employing the resilience indicator trends. Such metrics can be aggregated in preferably a hierarchical Bayesian Network to track the relative values and trends of Socio-Technical Organizational Resilience over time. This work will be further extended to develop corporate systems layer analysis and explore how IPSHA can be used to learn how the system will cope with failures and deviations under different conditions and to what extent the system can be stressed, both from technical and organizational viewpoints.

Appendix A: Resilience metrics

1. ED_1: Alarm rate
2. ED_2: Primary Containment Inspection or Testing Results Outside Acceptable Limits
3. ED_3: Number of unplanned maintenance jobs in a plant, requiring more than an hour to complete
4. ED_4: Mechanical database: $ED_{4\text{-}1}$: vibration analysis , $ED_{4\text{-}2}$: pump or seal leak analysis
5. ED_5: Process Safety Near-miss data
6. ED_6: Number of non-Tier 1 & 2 Loss of Primary Containment (LOPC) events
7. ED_7: Number of unplanned shutdowns per year
8. ETD_1: Demands on Safety system: $ETD_{1\text{-}1}$: Number of trips (SIL system activation) per month, $ETD_{1\text{-}2}$: Number of Pressure Relief Valve activations per month, $ETD_{1\text{-}3}$: Number of times mechanical device shutdown per month
9. ETD_2: % of time plant/process unit was operated outside design limits
10. ETD_3: % of changes executed through Management of Change procedure per year
11. P_1: Process Hazard Evaluations Completion
12. P_2: Process Safety Action Item Closure
13. P_3: Training Completed on Schedule - percentage of process safety required training sessions completed with skills verification
14. P_4: Procedures Current and Accurate- percent of process safety required Operations and Maintenance procedures reviewed or revised as scheduled
15. P_5: Work Permit Compliance
16. P_6: Safety Critical Equipment Inspection
17. P_7: Safety Critical Equipment Deficiency Management
18. P_8: Management of Change (MOC) and Pre Start-up Safety Review (PSSR) Compliance
19. P_9: Fatigue Risk Management
20. P_{10}: % of maintenance backlogs per quarter
21. P_{11}: Number of shift handover violations per year
22. P_{12}: Number of communications on learning from company or industry incidents
23. R_1: Number of tests for emergency systems and procedures per year
24. R_2: Number of mock drills for emergency situations per year

References

1. Aelion, V., & Powers, G. J. (1993). Risk reduction of operating procedures and process flowsheets. *Industrial & engineering chemistry research, 32*(1), 82-90.
2. Baybutt, P. (2002). Layers of protection analysis for human factors (LOPA-HF). *Process Safety Progress, 21*(2), 119-129.
3. Bruce K. Vaughen, K. B. (2016). Use the Bow Tie Diagram to help reduce process safety risks. (December 2016). http://www.aiche.org/resources/publications/cep/2016/december/use-bow-tie-diagram-help-reduce-process-safety-risks
4. Cagno, E., Caron, F., & Mancini, M. (2002). Risk analysis in plant commissioning: the Multilevel Hazop. *Reliability Engineering & System Safety, 77*(3), 309-323.

5. Cameron, I., Hangos, K., Lakner, R., Nemeth, E., & Seligmann, B. (2007). *The P3 formalism: A basis for improved diagnosis in complex systems.* Paper presented at the Chemeca 2007: Academia and Industry Strengthening the Profession.
6. Cameron, I., Seligmann, B., Hangos, K., Németh, E., & Lakner, R. (2008). *A functional systems approach to the development of improved hazard identification for advanced diagnostic systems.* Paper presented at the ESCAPE-18 Conference.
7. Cheung, J.-Y., & Stephanopoulos, G. (1990). Representation of process trends—Part I. A formal representation framework. *Computers & Chemical Engineering, 14*(4), 495-510.
8. Chudleigh, M., & Clare, J. (1993). The benefits of SUSI: Safety analysis of user system interaction *SAFECOMP'93* (pp. 123-132): Springer.
9. Crowl, D. A. (2007). *Human factors methods for improving performance in the process industries*: John Wiley & Sons.
10. Dunjó, J., Fthenakis, V., Vílchez, J. A., & Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials, 173*(1), 19-32.
11. Eckerman, I. (2005). *The Bhopal saga: causes and consequences of the world's largest industrial disaster*: Universities press.
12. Flin, R. (2001). Decision making in crises: The Piper Alpha disaster. *Managing crises: Threats, dilemmas, opportunities*, 103-118.
13. Flin, R., Mearns, K., Gordon, R., & Fleming, M. (1996). Risk perception by offshore workers on UK oil and gas platforms. *Safety science, 22*(1), 131-145.
14. Galán, S. F., Mosleh, A., & Izquierdo, J. (2007). Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models. *Reliability Engineering & System Safety, 92*(8), 1131-1138.
15. Giardina, M., & Morale, M. (2015). Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology. *Journal of loss prevention in the process industries, 35*, 35-45.
16. Gressel, M. G., & Gideon, J. A. (1991). An overview of process hazard evaluation techniques. *The American Industrial Hygiene Association Journal, 52*(4), 158-163.
17. Hoepffner, L. (1989). Analysis of the HAZOP study and comparison with similar safety analysis systems. *Gas Separation & Purification, 3*(3), 148-151.
18. Hollnagel, E., Nemeth, C. P., & Dekker, S. (2008). *Resilience engineering perspectives: remaining sensitive to the possibility of failure* (Vol. 1): Ashgate Publishing, Ltd.
19. Hollnagel, E., Woods, D. D., & Leveson, N. (2007). *Resilience engineering: concepts and precepts*: Ashgate Publishing, Ltd.
20. Holmstrom, D., Altamirano, F., Banks, J., Joseph, G., Kaszniak, M., Mackenzie, C., . . . Wallace, S. (2006). CSB investigation of the explosions and fire at the BP Texas City refinery on March 23, 2005. *Process Safety Progress, 25*(4), 345-349.
21. Huang, S., Chiu, C.-H., & Elliot, D. (2007). *LNG: Basics of liquefied natural gas*: University of Texas Continuing Education Petroleum Extension Service.
22. Jackson, S. (2009). *Architecting resilient systems: Accident avoidance and survival and recovery from disruptions* (Vol. 66): John Wiley & Sons.
23. Jain, P., Pasman, H. J., Waldram, S. P., Rogers, W. J., & Mannan, M. S. (2016). Did we learn about risk control since Seveso? Yes, we surely did, but is it enough? An historical brief and problem analysis. *Journal of loss prevention in the process industries*.
24. Janusz, M. E., & Venkatasubramanian, V. (1991). Automatic generation of qualitative descriptions of process trends for fault detection and diagnosis. *Engineering Applications of Artificial Intelligence, 4*(5), 329-339.
25. Kariuki, S., & Löwe, K. (2007). Integrating human factors into process hazard analysis. *Reliability Engineering & System Safety, 92*(12), 1764-1773.
26. Katz, D., & Kahn, R. L. (1978). The social psychology of organizations.
27. Kennedy, R., & Kirwan, B. (1998). Development of a hazard and operability-based method for identifying safety management vulnerabilities in high risk systems. *Safety science, 30*(3), 249-274.
28. Khan, F., Rathnayaka, S., & Ahmed, S. (2015). Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection, 98*, 116-147.
29. Khan, F. I., & Abbasi, S. (1997a). OptHAZOP—an effective and optimum approach for HAZOP study. *Journal of loss prevention in the process industries, 10*(3), 191-204.
30. Khan, F. I., & Abbasi, S. (1997b). TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner. *Journal of loss prevention in the process industries, 10*(5), 333-343.
31. Khan, F. I., & Abbasi, S. (1999). Major accidents in process industries and an analysis of causes and consequences. *Journal of loss prevention in the process industries, 12*(5), 361-378.
32. Khan, F. I., & Abbasi, S. (2000). Towards automation of HAZOP with a new tool EXPERTOP. *Environmental Modelling & Software, 15*(1), 67-77.
33. Kleiner, B. M. (2006). Macroergonomics: analysis and design of work systems. *Applied Ergonomics, 37*(1), 81-89.
34. Kletz, T. A. (2001). *Learning from accidents*: Routledge.
35. Knowlton, R. E. (1987). Introduction to hazard and operability studies: the guide word approach *Introduction to hazard and operability studies: the guide word approach*: Chemetics International Company.
36. Lawley, H. (1974). Operability studies and hazard analysis. *Chemical Engineering Progress, 70*(4), 45-56.
37. Le Coze, J.-C. (2008). *BP Texas city accident: weak signal or sheer power?* Paper presented at the 3. Resilience Engineering Symposium.

38. Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural hazards review, 14*(1), 29-41.
39. Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science, 42*(4), 237-270.
40. Nimmo, I. (1993). Start up plants safely. *Chemical Engineering Progress, 89*(12), 66-70.
41. Palmer, C., & Chung, P. (2008). A computer tool for batch hazard and operability studies. *Journal of loss prevention in the process industries, 21*(5), 537-542.
42. Pasmore, W. A., & Sherwood, J. J. (1978). *Sociotechnical systems: A sourcebook*: Pfeiffer & Co.
43. Pate-Cornell, M. E. (1993). Learning from the piper alpha accident: A postmortem analysis of technical and organizational factors. *Risk Analysis, 13*, 215-215.
44. Pittman, W., Han, Z., Harding, B., Rosas, C., Jiang, J., Pineda, A., & Mannan, M. S. (2014). Lessons to be learned from an analysis of ammonium nitrate disasters in the last 100 years. *Journal of hazardous materials, 280*, 472-477.
45. Raman, J., Gargett, A., & Warner, D. (1991). *Application of Hazop techniques for maintenance safety on offshore installations.* Paper presented at the SPE Health, Safety and Environment in Oil and Gas Exploration and Production Conference.
46. Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety science, 27*(2), 183-213.
47. Rathnayaka, S., Khan, F., & Amyotte, P. (2011a). SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. *Process Safety and Environmental Protection, 89*(3), 151-164.
48. Rathnayaka, S., Khan, F., & Amyotte, P. (2011b). SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study. *Process Safety and Environmental Protection, 89*(2), 75-88.
49. Reason, J. (1990). *Human error*: Cambridge university press.
50. Reiman, T., & Rollenhagen, C. (2014). Does the concept of safety culture help or hinder systems thinking in safety? *Accident Analysis & Prevention, 68*, 5-15.
51. Rengaswamy, R., & Venkatasubramanian, V. (1995). A syntactic pattern-recognition approach for process monitoring and fault diagnosis. *Engineering Applications of Artificial Intelligence, 8*(1), 35-51.
52. S.W. Ostrowski, K. K. (2008). A HAZOP Methodology for Transient Operations.
53. Schurman, D. L., & Fleger, S. A. (1994). Human factors in HAZOPs: Guide words and parameters. *Professional Safety, 39*(12), 32.
54. Seligmann, B., Németh, E., Hockings, K., McDonald, I., Lee, J., O'Brien, C., . . . Cameron, I. (2010). *A structured, blended hazard identification framework for advanced process diagnosis.* Paper presented at the 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industries (Loss Prevention 2010).
55. Srinivasan, R., & Venkatasubramanian, V. (1996). Petri net-digraph models for automating HAZOP analysis of batch process plants. *Computers & Chemical Engineering, 20*, S719-S725.
56. Srinivasan, R., & Venkatasubramanian, V. (1998a). Automating HAZOP analysis of batch chemical plants: Part I. The knowledge representation framework. *Computers & Chemical Engineering, 22*(9), 1345-1355.
57. Srinivasan, R., & Venkatasubramanian, V. (1998b). Automating HAZOP analysis of batch chemical plants: Part II. Algorithms and application. *Computers & Chemical Engineering, 22*(9), 1357-1370.
58. Stephans, R. A. (2012). *System safety for the 21st century: The updated and revised edition of system safety 2000*: John Wiley & Sons.
59. Sundarraman, A., & Srinivasan, R. (2003). Monitoring transitions in chemical plants using enhanced trend analysis. *Computers & Chemical Engineering, 27*(10), 1455-1472.
60. Suokas, J. (1988). The role of safety analysis in accident prevention. *Accident Analysis & Prevention, 20*(1), 67-85.
61. Suokas, J., & Rouhiainen, V. (1989). Quality control in safety and risk analyses. *Journal of loss prevention in the process industries, 2*(2), 67-77.
62. Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis, 11*(3), 499-507.
63. Tauseef, S., Abbasi, T., & Abbasi, S. A. (2011). Development of a new chemical process-industry accident database to assist in past accident analysis. *Journal of loss prevention in the process industries, 24*(4), 426-431.
64. Taylor, J. (2013). Incorporating human error analysis into process plant safety analysis. *Chem Eng Trans, 31*, 301-306.
65. Trist, E., & Bamforth, K. (1951). Some social and psychological consequences of the Longwall method. *Human relations, 4*(3), 3-38.
66. Venkatasubramanian, V., Zhao, J., & Viswanathan, S. (2000). Intelligent systems for HAZOP analysis of complex process plants. *Computers & Chemical Engineering, 24*(9), 2291-2302.
67. Viswanathan, S., Shah, N., & Venkatasubramanian, V. (2000). A hybrid strategy for batch process hazards analysis. *Computers & Chemical Engineering, 24*(2), 545-549.
68. Viswanathan, S., Zhao, J., Venkatsubramanian, V., Mockus, L., Vinson, J., Noren, A., & Basu, P. K. (1999). Integrating operating procedure synthesis and hazards analysis automation tools for batch processes. *Computers & Chemical Engineering, 23*, S747-S750.
69. Wang, F., Gao, J., & Wang, H. (2012). A new intelligent assistant system for HAZOP analysis of complex process plant. *Journal of loss prevention in the process industries, 25*(3), 636-642.
70. Weick, K. E., & Sutcliffe, K. M. (2011). *Managing the unexpected: Resilient performance in an age of uncertainty* (Vol. 8): John Wiley & Sons.
71. Willey, R. J., Hendershot, D. C., & Berger, S. (2007). The accident in Bhopal: observations 20 years later. *Process Safety Progress, 26*(3), 180-184.

72. Zhao, D., McCoy, A. P., Kleiner, B. M., Smith-Jackson, T. L., & Liu, G. (2015). Sociotechnical systems of fatal electrical injuries in the construction industry. *Journal of Construction Engineering and Management, 142*(1), 04015056.