MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Assessment of Hazard Analysis and Implementation of STPA in Process Industry

Parveen Chahal, Javeed I Mohammed
Fluor Canada Ltd.
*Presenters E-mails: *christina.ng@fluor.com, javeed.mohammed@fluor.com, parveen.chahal@fluor.com,

Abstract

High-performance computing has changed the world on its head with capabilities of image processing and artificial intelligence. The world of Energy and chemical has also changed with the adoption of these highly complex computing power and software capabilities of the modern processors by adoption of smart measurement technology (in sensors and final elements) and development of complex software algorithms. The modern technology has helped to put the plants to optimum level of operation and close to design margins to maximize profitability, which resulted in adding to the complexity of process control strategies.

With the advent of complex software capabilities the understanding the flaws in the specification and hazard identification process is not well understood.

Process Industry uses many available tools / techniques for HAZARD identification but many of these techniques predate to the advent of these advancement being made in the computer technology. Industry uses international performance based standards viz. IEC 61508/61511 which do provide guidelines to eliminate the "systematic errors" that may propagate through the design of the safety systems life cycle and render the safety system useless in certain modes of operation. Still there have been many incidents /near misses that have the potential to cause hazard to the People, Asset and environment which highlights that there is a plank missing which can help and reduce the number of incidents by designing more robust safety systems.

STAMP model address these concerns which indicate that "the safety related incidents can be related to flaws in requirement specification" (Prof. Nancy Leveson)

1. Introduction

The concept of process safety has come to the forefront of Energy and Chemical industry due to various incidents like Flixborough, Piper Alfa, BP Texas city and has become norm

for operating companies, being required by legislation as well as by industry standards. The industrial standards, rather than being prescriptive, are performance based. The industry however still adheres to proven safety codes like NFPA-85 for boiler and combustion safety.

In Energy and chemical industry the process safety is managed as follows

- Structured study for the Identification of Hazards (eg. HAZOP)
- Allocation of safety function to protection layers viz. Quantitative / qualitative risk analysis (eg. FTA, Risk Matrix, LOPA etc.)
- Design and Engineering of Safety System: SIL level design verification including verification of systematic capability to address interactions within different components of the subsystem.
- Installation, commissioning and validation of the safety system for continued reliability of operation
- Management of changes in design and impact analysis of the changes

The backdrop to this view of process safety has been implementation of high-performance computing which changed the world on its head with capabilities of image processing and artificial intelligence. The world of Energy and chemical has also changed with the adoption of these highly complex computing power and software capabilities of the modern processors by adoption of smart measurement technology (in sensors and final elements) and development of complex software algorithms. The modern technology has helped to put the plants to optimum level of operation and close to design margins to maximize profitability, which resulted in adding to the complexity of process control strategies.

With the advent of complex software capabilities the understanding the flaws in the specification and hazard identification process is not well understood.

Process Industry uses many available tools / techniques for HAZARD identification but many of these techniques predate to the advent of these advancement being made in the computer technology. Industry uses international performance based standards viz. IEC 61508/61511 which do provide guidelines to eliminate the “systematic errors” that may propagate through the design of the safety systems life cycle and render the safety system useless in certain modes of operation. Still there have been many incidents /near misses that have the potential to cause hazard to the People, Asset and environment which highlights that there is a plank missing which can help and reduce the number of incidents by designing more robust safety systems.

1.1 Present state of the industry in Hazard Analysis and Identification

Hazard identification is first and most important activity of the safety life cycle and lays the foundation stone of the Safety System. Hazard & Operability study (HAZOP) has been

an integral part of identifying the Hazard in process plants. This HAZARD identification or design verification process have been adopted in response to various disaster in process industry which involved significant plant damage, environmental damage and worse of them all being loss of lives.

So application of Hazard identification in process industry has almost been a knee jerk reaction. It is seen as one the critical (and payment) milestone on the project schedule. The HAZOP ToR(term of reference) is a key document which is developed by HSE, Process Engineering and Safety Engineering department. The final outcome of this painstaking, multidisciplinary brain-storming exercise is to identify the risks in the process and also identify (or design) the safeguards that are appropriate for risk as determined by risk ranking of the Hazards. Due to the sheer nature and process of HAZOP, it is generally done on mature designs. However there are various other analytical methods which can be implemented in Hazard Identification like

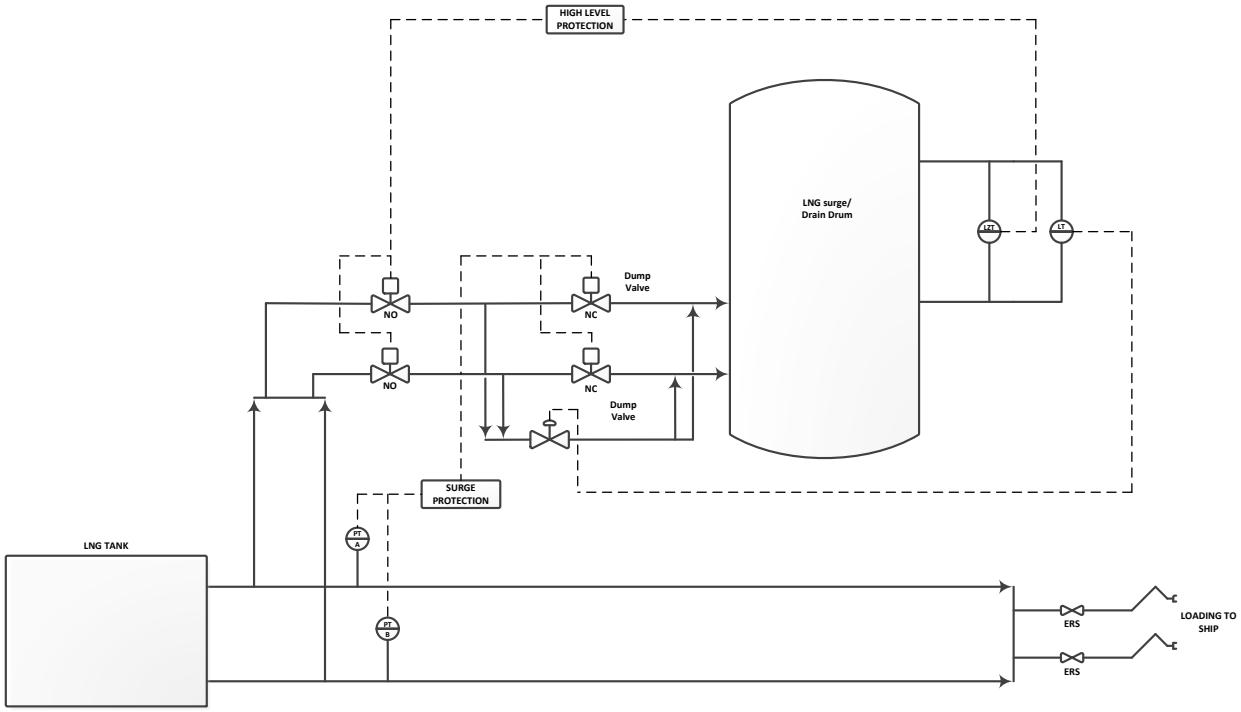
- What-If Analysis
- Failure Modes and Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Bow-tie analysis

From traditional execution point of view, HAZOP can be seen as a formal audit, or design verification tool of an essentially mature design. So HAZOP relies on the overall design process to properly consider hazards, risk and safeguards. The next step in the life cycle is to conduct Layer of Protection Analysis (LOPA) which identifies the independent protection layers to guard against the hazard. The safeguards shall being identified during the LOPA analysis shall be Specific, Independent, Dependable and Auditable.

1.2 Case Study – LNG Tank Loading

LNG storage tank continuously receives rundown LNG from the LNG trains. LNG is stored in storage tank and is shipped to the Jetty via 2 redundant lines (approx. 1.5 km away). There are 2 modes of operation:

- Holding Mode – In this mode the LNG is circulated to the Jetty for cold keeping and to prevent vapor accumulation in loading line. The LNG goes through one header and returned through the other. Only 1 LNG loading pump (inside the LNG tank) is running during this mode.
- Loading Mode – In this mode LNG is pumped from the LNG storage tank and loaded into an LNG carrier through redundant loading lines.



LNG Loading

During normal operation a small fraction of LNG is also routed to the LNG drain / Surge Drum to maintain the drum at the operating temperature. The level inside the drum is maintained by level controller via control valve which is located on the bypass line of the Normally Closed Dump Valves.

During loading mode the if there is an emergency at the Jetty, Loading arm or at the ship the Emergency Release System (ERS) valves are closed within 5 seconds to prevent damage to the loading arms. Some of the safeguards are as follows:

Excessive movement of the loading arm will close the ERS valves and open the normally closed Dump Valves within 5 second matching the closing time of the ERS valves.

Emergency shutdown at the ship will also initiate the closure of ERS and also opens the dump valve within 5 seconds

Activation of ERS will result in high pressure on the LNG loading lines, which will be detected by the pressure transmitters which in turn will activate the surge protection and open the dump valve in 5 seconds.

High-high level inside the Drain / Surge Drum will initiate high high level protections and close the valves upstream of the dump valves and also trip the LNG pumps.

1.3 Incident

In case of activation of ESD from ship the ERS valves closed in 5 seconds and activated the surge protection which opened the dump valve in 5 seconds. The level inside the Drain/

Surge vessel rises instantaneously to high-high level and initiated the high-high level protection. This protective function closed the valves upstream of the dump valve which conflicted with the design intent of the surge protective function and resulted in aborting the surge protection.

In the above example all the functions performed as designed but there was a systematic error in the design which could not be identified by conventional HAZOP technique due to the inherent nature of how HAZOP is conducted.

2. Missing link and expert analysis

There is no substitute for expert thought; providing that thought, however, is easy to say, but hard to do.

Some barriers to the kind of careful, expert thought; which is needed for effective systems theoretic implementation that are addressed in the paper are:

- Time constraint, lack of skills and retiring of experts
- Risk and the problem of scale
- Countervailing effect of advancements in engineering

2.1 Time constraint, lack of skills and retiring of experts

Not very long ago majority of the big Oil and Gas operating companies had quite a large number of experts who were engaged in projects and were available for resolving complex problems. Majority of these groups are now dismantled or dissolved due to restructuring within the organizations and/or cost reasons and/or retiring of the experts in task force. The current situation is that fairly inexpert personnel in the organization are trying to solve these problems by applying complex – typically performance based -standards that they understand fairly poorly. As a result many of the big operating companies prepared heavily prescriptive engineering specifications. But even the best standards require a considerable level of understanding and cannot be used as a replacement of the experience. Many of the personnel in the projects are new to the organization and do not completely understand the intent behind these specifications. Lack of understanding of specifications coupled with fast paced schedules has made the situation even worse.

2.2 Risk and the problem of scale

Risk appetite is function of organizational scale. For a big multinational Oil and Gas organization, operating plants at multiple plants across the globe, the impact of releasing a hazard or catastrophe is quite high, but for a small operating company the impact of a Hazard is not huge. Hence smaller companies do not have much of an incentive to carefully evaluate the risk in their plants.

The risk matrices perform poorly at the edges which reflect frequent-but-trivial and catastrophic-but-rare. So using these matrices at the extremes can provide either highly over rated systems (more CAPEX and OPEX) or under specified systems. Big operating

companies generally use more sophisticated and quantitative analysis for such high consequence e scenario to properly asses the Hazard in the process and optimizes the design. Smaller organization on the other hand does not see potential benefits out of it.

So these two considerations indicate that large organizations are likely to see more potential benefits of systems theoretic approach.

2.3 Countervailing effect of advancements in engineering and corporate policies

It might seem that the large organizations have higher incentives in implementing the Systems theoretic implementation but – Don't count your chickens before they hatch.

Large organizations have technical experts who work with more stringent safety standards which provide proven guidance on implementation of these standards with proven outcomes.

Also bigger organizations have corporate safety policies which place onus on safety first and value safety more than the production. These policies are part of corporate safety culture and have been proven by test of time.

As a result, surprisingly, big organizations also have less incentive to adopt new approaches.

3. Traditional process safety and systems theoretic approach

Highly sophisticated and new hazard analysis technique like Systems Theoretic Process Analysis (STPA) and Causal Accident Systems Theoretic (CAST) which are based on an extended model of accident causation are widely applied in aerospace and automobile sector and can be applied to process industry but the focus here is on how to apply the systems theoretic approach on the already available methods in process industry.

3.1 Opportunities in quantitative and semi-quantitative methods

There are various quantitative and semi-quantitative techniques available but the most commonly used techniques are LOPA and Bow-tie. LOPA is a semi-quantitative analysis and is a simplified method of risk assessment that provides much needed middle ground between qualitative hazard analysis and traditional, quantitative analysis.

LOPA provides a chain of event leading to the Hazard and may not be the best tool for analyzing all the hazardous event outcomes but these this tool can be used a starting point which can combine the simplicity with a meaningful level of analysis. LOPA can be used to change the perception of risk that one evaluates in qualitative reviews like HAZOP to a more scientific approach like STPA. It can be used a first step towards such a transition.

Bow-tie on the other hand is not being currently used many organization in process industry. The ones who use this technique do not the understand power of this tool and merely use it as verification tool to count the barriers leading to a hazard. Bow-tie can analyze multiple initiating scenarios and multiple consequences at same time which can be

the tool used to analyze more complex scenarios and transition from traditional approach to scientific approach.

3.2 Alarm objective Analysis

With the advent of sophisticated control systems and advance computing capabilities more complex logic can be implemented but this also resulted in unnecessary complexities and operability issues.

More and more alarms are being added sometimes even when not necessary which subsequently results in unnecessary nuisance and overwhelming the operator and diverting attention from important issues during an emergency or shutdown. Majority of the alarms are recommended during the HAZOPs as the team assessing the design thinks it as a good to have feature. Later in the project during the Alarm rationalization workshops majority of these alarms are deleted. This is a clear indication that the team involved in providing these kinds of recommendation does not understand the implications of adding so many alarms and fully understand the process.

The process of alarm rationalization itself is an activity which can help in understanding the operation of the plant from a system engineering approach rather than the conventional approach used during the conventional methods lie HAZOP and can be viewed as a step in transitioning towards systems model.

4. Implementation in Energy & Chemicals

Hazards present in Energy & Chemicals are different from other industries where STAMP model have been implemented. The following factors are unique to process sector.

4.1 Multiple failures and Global Acceptance

Majority of failures in process industry are not due to a single component failures but are a result of multiple component failures which interact with each other and loss of containment being at the center of the multi-casualty incidents. As a result the professional believe that reliability and availability model are best models for identification of hazards especially with limited expertise with in the industry. Many NoBo (Notified bodies) and standards like IEC 61511 ask for a functional safety assessment (FSA) complying with the local regulations or with international standards before the startup. Convincing the end users and these regulators to accept a new technique like STPA will take some time.

4.2 Designers and Operators

EPC companies are involved in the designing of the plants are not involved in the operation of the plant. They can provide guidance and provide recommendation to the end user to operate the plant within safe design criteria. So once the plant is handed over to the end-user they have no control or ability to prevent the system to migrate to higher risk state or beyond the safe design limits

5. Conclusion

Looking into the kind of techniques currently used in process industry it does represent an advance in the opinion on how the risk is assessed and managed. Over time the there is a potential to insert more rigorous technologies like STAMP models to identify the Hazards. Adapting to these new models will guide the operating companies on how to operate the plants within the constraints identified in the design.