Comparative Analysis of Hazard and Operability Study (HAZOP) and Systems Theoretic Process Analysis (STPA)

The objective of the study described in this paper was to evaluate and compare STPA with the standard HAZOP method commonly used for Process Hazard Analysis (PHA). Both methods were applied by independent and qualified expert teams to discover flaws in a real system. Neither team had any preexisting knowledge of flaws before applying the methods. The system contained real flaws that led to adverse events during the operation of the system. The outcomes and recommendations of HAZOP and STPA are compared to determine what differences exist, if any, and identify whether critical gaps exist for modern process industry applications. The HAZOP and STPA results are also compared to the corrective actions produced after the hazardous and costly incident during operation. The STPA method was found to capture hazardous human and automation related behaviors that were missed by HAZOP, and STPA generated critical recommendations missed by HAZOP that would have prevented the real adverse events. The STPA results anticipated the causes and corrective actions that were otherwise only discovered after the hazardous and costly event during system operation.

Faisal Jamal, Kamran Arif, Arooba Arooj
Corporate HSE & Technical Services, Fatima Group, Pakistan

Dr. John P. Thomas
Engineering Systems Lab, Massachusetts Institute of Technology (MIT), USA

Introduction

Major incidents involving hazardous chemicals that are toxic, reactive, explosive, or flammable continue to occur throughout the process industries despite the use of standard methods to prevent such incidents. Investigations identify proximal causes and produce corrective actions to address weaknesses that were discovered only after significant losses occurred. Rarely does the investigation go far enough to ask why the hazard analysis failed to identify the weaknesses or failed to implement effective corrective actions before the system was put into operation. Do standard hazard analysis methods like HAZOP have critical weaknesses that overlook certain types of causes or interactions? Can alternative methods like STPA produce more effective results given the same information before an incident? This paper compares HAZOP and STPA, including empirical results from two expert teams that applied each method.

Background

Overview of Preventable Incidents

Major incidents have been happening for decades. A 1974 incident in Flixborough, Lincolnshire, England [1] resulted in 28 deaths and 36

injuries. A 1984 incident in Bhopal, India [2] resulted in more than 2,000 deaths. A 1989 incident at Phillips Petroleum Company, Pasadena, USA [3] resulted in 23 deaths and 314 injuries. A 1990 incident at BASF, Cincinnati, USA [4], resulted in 1 death and 71 injuries. A 1991 incident at IMC, Sterlington, USA [5], resulted in 8 deaths and 120 injuries. A 2005 explosion at Texas City Refinery, USA [6] resulted in 15 deaths and 180 injuries. A 2010 incident on the Deepwater Horizon, USA [7] resulted in 11 deaths and the largest marine oil spill in history. A 1976 Ammonia loading line rupture at Swedish Fertilizer Company [8], resulted in 2 deaths. Meanwhile, many more minor incidents continue to occur in the process industries.

This study evaluates gaps in the popular HAZOP-based hazard analysis as performed by professional teams on real applications and compares the results to STPA-based hazard analysis also performed by professionals on real applications. The results are compared to real loss events experienced during operation of the system that were unknown to both teams.

Hazard and Operability Study (HAZOP)

HAZOP is one of the most utilized Process Hazard Analysis (PHA) techniques and is an important element of OSHA Process Safety Management (PSM). HAZOP plays a pivotal role in identification, evaluation and control of all possible hazards involved in the oil & gas and petrochemical process industry which may lead to catastrophic events such as loss of primary containment, fire, explosion, injuries and / or environmental excursions.

The HAZOP technique was introduced in the 1963. Later, it was further developed by ICI and Chemical Industries Association in the early 1970s, however the technique only started to be more widely used within the chemical process industry after the Flixborough disaster in 1974. Over time, the importance of risk management and the acceptance of HAZOP grew throughout the chemical industry. HAZOP eventually became a global standard with IEC 61882 [9].

HAZOP is based on the idea that risk events are caused by deviations from design or operating intent. Deviations are identified by using guide words such as “more”, “less”, or “reverse” flow. This approach can help stimulate the imagination of team members when exploring potential deviations. The HAZOP technique has been useful in the process industries to identify potential hazards and causes and to identify necessary mitigations to prevent them.

A number of HAZOP modifications have been proposed in the literature, but none of these have led to widespread industry adoption to the extent HAZOP has. Modifications include Computer HAZOP (CHAZOP) [10], Safety Culture Hazard and Operability (SCHAZOP) [11], Human HAZOP [12], and Programmable Electronic System HAZOP (P.E.S. HAZOP) [13].

System Theoretic Process Analysis (STPA)

System Theoretic Accident Model and Process (STAMP) is a novel accident causality model based on systems theory and systems thinking [14]. It integrates into engineering analysis the causal factors in our increasingly complex systems such as software, human-decision making and human factors, new technology, social and organizational design, and safety culture. System Theoretic Process Analysis (STPA) is a hazard analysis method based on the STAMP model.

STPA has been adopted on a wide range of applications across several industries including nuclear power [15], nuclear weapons [16], oil & gas [17], aviation [18], automotive and autonomous vehicles [19], and others to control new hazards caused by complex software, incorrect engineering assumptions, unsafe automated behaviors, human interactions, and dysfunctional interactions between systems.

STPA considers component failures and deviations from design intent, but also considers unsafe behaviors that match the design intent with or without a deviation. Examples include components that correctly satisfy all requirements (but

the requirements are incomplete or incorrect), components individually work as designed but collectively interact in unsafe ways, humans that follow defined rules and procedures (but the rules and procedures are incomplete or incorrect), or a flawed design or operating intent that is based on incorrect assumptions about the system or the environment. STPA anticipates losses that are caused by unsafe *interactions* of system components with or without a deviation.

Organizations that have adopted STPA report several advantages over traditional hazard/risk analysis techniques including:

1. Capability to analyze very complex systems in less time
2. "Unknown unknowns" that were previously only found in operations can be identified in the development process and either eliminated or mitigated.
3. Ability to begin earlier in concept development to assist in identifying safety requirements and constraints. These can then be used to
   a) Design safety (and security) into the system architecture
   b) Eliminate costly rework involved when design flaws are identified late in development or during operations.
4. Maintaining complete traceability from requirements to all system artifacts, enhancing system maintainability and evolution.
5. Coverage of software behaviors and human operators in one unified analysis. Neither is analyzed in isolation, ensuring a more comprehensive analysis that considers environmental and contextual factors that lead to losses.
6. STPA provides a common easy-to-understand format that documents system functionality that is often missing or difficult to find in large, complex systems.
7. STPA can be easily integrated into the system engineering process and into model-based system engineering.

Comparison Methodology

This study compares results from HAZOP and STPA performed on a real complex application by qualified professionals.

A real fertilizer plant application with both automated and human controls was selected. The application was analyzed by a qualified HAZOP team before commissioning and operation. However, an incident occurred on the HAZOP-ed application.

STPA was performed on the same system to identify the weaknesses. Each team included qualified method experts with appropriate training and over a decade of industry experience applying the selected method.

The application contained weaknesses and flaws that were recognized after it was put into operation. Both analysis teams were blind to the weaknesses and the operational events, with no knowledge of either when they performed the hazard analysis. Both teams were limited to general design information available before the application was put into operation.

Case Study Selection

A study of fertilizer plants and past incidents was conducted to understand the types of causes that have not been adequately prevented by HAZOP in the past and to help select a candidate application to evaluate the differences between HAZOP and STPA.

Fertilizer plant incidents published in American Institute of Chemical Engineers (AIChE) Technical Manuals and other sources were surveyed to identify past incidents. A study of 30 years of incidents revealed that the underlying causes of were directly or indirectly linked with gaps in the HAZOP exercise. A summary of a few of the reported events is provided in Table 1 below.

Table 1: Summary of Various Reported Events involving HAZOP-ed Processes [20]			
SN	**Incidents**	**Year**	**Root cause**
1	Failure of Level Bridle in Benfield Service	2016	Mechanical overload due to localized internal corrosion as per the Materials analysis. The process safety review however looked at the lack of the HAZOP to identify the presence of the corrosive liquid in the bridle.
2	Explosion of an aqueous Ammonia scrubber tank	2010	Explosion of a trapped hydrogen/air mixture which had accumulated in dead pockets of the aqueous ammonia scrubber tank. Incomplete/inaccurate HAZOP did not address this risk.
3	Foaming of Catacarb™ CO_2 Removal System leads to Methanator Runaway Reaction and Expander Fire Incident	2015	Methods for analyzing Suspended solids misguided the operational staff. No built in Expander Trip Logic upon closure of Methanator inlet valve caused no seal gas availability and process gas ingress into Expander Oil Console caused fire incident.
4	Catastrophic Explosion in the CO_2 Removal Unit of an Ammonia Plant	2015	Reverse flow of amine solution due to absence of check valves resulted in explosion.
5	Explosion of a Benfield Solution Storage Tank	1985	Hydrogen gas entered the Benfield solution storage tank combining with sufficient oxygen and was ignited by a static charge causing complete destruction of the tank.
6	Failure of Methanator Feed Effluent Exchanger Tubes due to Benfield Solution Carry over from CO_2 Absorber	2014	Absorber Demisters design failure. Low load operation resulting in bypassing of demisters. The gas washing system of Absorber KOD not in continuous service.
7	Failure of Semi-Lean Catacarb Pump due to Reverse flow	2004	Reverse flow of process gas resulting in the reverse rotation of the pump leading to catastrophic failure of pump and driver.
8	Case Study of CO_2 Removal System Problems/Failures	1999	Casing vanes of hydraulic turbines were found to be eroded due to wrong location of valve.
9	Explosion of Hydrogen in a Pipeline for CO_2	2001	Hydrogen enriched gas had entered the pipeline, nitrogen purge had not been effective, air had leaked into the line and formed an explosive mixture, and the mixture had ignited.
10	Failure of NG compressor train	2002	Install an additional trip valve at the inlet steam line of turbine. Also recommended detailed HAZOP of turbomachinery.

HAZOP is popular but not perfect and costly incidents still happen in HAZOP-ed processes. Common HAZOP limitations identified from these events include limited consideration of automation behavior, human factors and interactions between subsystems, components, or nodes.

Comparative Analysis: HAZOP & STPA

A case study was selected based on a real system at Fatima Fertilizer Limited (FFL). Health, Safety and Environment (HSE) is the high priority of our operations. FFL is a Guinness World Records title holder setting a new standard of safe operations with more than 66 million safe man-hours as of 31 March 2022 - the highest in the global fertilizer industry. The team is committed to continuous improvement and innovation in the HSE performance. Thus, FFL was selected as an ideal candidate to provide the resources needed to compare HAZOP and STPA on a real system.

CO_2 removal system with automated and human controls was selected to share the findings of the comparative analysis in this paper. FFL met all industry standard practices for conducting the HAZOP study as a part of detailed engineering and implementation of the recommendations.

History of FFL Ammonia Plant

The FFL Ammonia plant operating at Sadiqabad, Pakistan was designed by CF Braun & Co. Alhambra California (purifier technology) and built in 1967. This Plant was initially operated by Exxon. It was later bought by Kemira in 1985 and kept the same operational philosophy with exemplary service factor. This plant was shut down in 2000 for business reasons. FFL relocated it from the Netherlands to Pakistan in 2007 and started successful production in 2010.

Description of CO_2 Removal System

CO_2 removal is a vital process (Figure 1) in Ammonia manufacturing as CO_2 present in raw Syn Gas is a poison for Ammonia synthesis catalyst. In the FFL plant CO2 is removed by absorption in potassium carbonate solution (~30% by weight) in proprietary Catacarb^{TM} process. The absorber tower consists of two packed sections. In the lower section, the gas is scrubbed with semi-lean Catacarb solution. In the upper section, lean solution is used to remove CO_2. Process Gas is distributed beneath the bottom packed beds. The lean and semi-lean Catacarb streams are sprayed into the tower over the packed beds. Purified Gas flows from the top of the tower to a knockout drum (KOD) and the carried-over liquid is drained from the bottom of the KOD to the drain system for recovery via a level controller. Purified Gas from the top of the KOD is sent to the Methanator to further remove the oxides to ppm level in Ammonia synthesis gas. Rich Catacarb solution from the hydraulic turbine flows into the top section of the CO_2 stripper. The regeneration of Catacarb solution also takes place in two stages with semi-lean solution being pumped out halfway down the stripper and the lean solution from the base. In the stripper tower, the rich Catacarb solution is stripped by depressurization and by heating with steam vapors generated by reboilers at the base of the tower. The rich solution passes through a hydraulic turbine to partially recover pumping power for the semi-lean pump which pumps the semi-lean solution from middle section of the stripper to midway up the absorber column. The lean solution is pumped from bottom of the stripper tower to the top of the absorber column

Incident Description [21]

On 29th August 2012, Ammonia plant was in restart phase after 10 days of planned shutdown. Various problems were encountered including foaming in Catacarb causing excessive and repeated solution carryover to Methanator. On 3rd September, Methanator temperature increased beyond the trip limit of 806°F (430°C) but Methanator trip logic did not actuate automatically due to its built-in selector switch option on DCS HMI (Human Machine Interface), provision of selecting 1oo4 is provided in build in design for logic actuation. Once it was observed that temperature reached to 960°F (516°C), Methanator inlet valve HV-25 was immediately closed by operators, cutting downstream seal gas flow towards the Expander. The inlet valve HV-25 was designed to close automatically in emergency situations. In addition, there was no built-in Expander Trip Logic to respond in the event of closure of Methanator inlet valve HV-25, which resulted in no seal gas flow and process gas ingress into Expander Oil Console. Cold box Expander process gas broke through from HP drain to oil console causing console over pressurization and resulted in hydrogen fire. Issues were resolved one by one by taking appropriate engineering controls and operational measures. Production resumed on 15th September 2012.

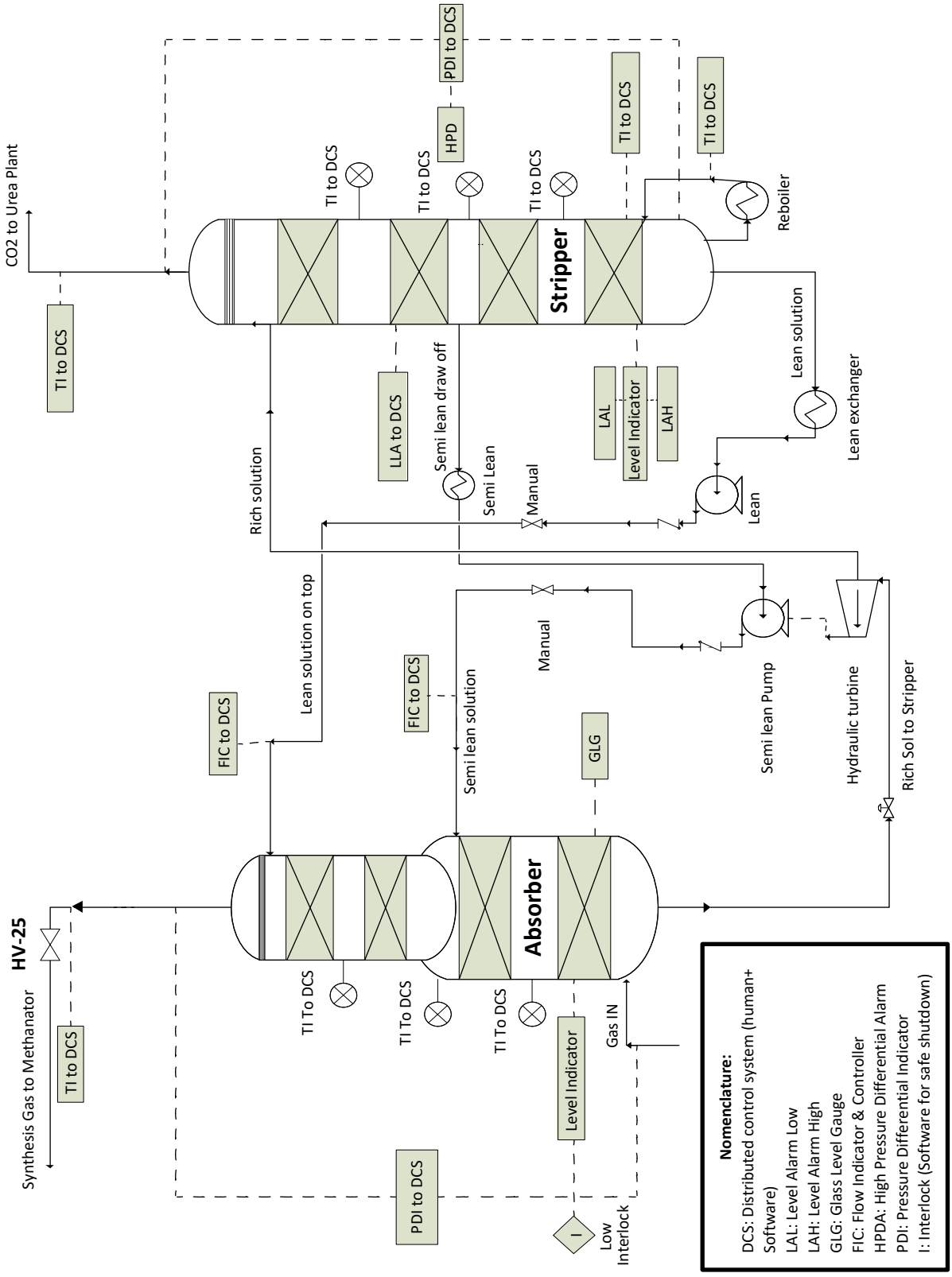

Figure 1: Catacarb^{TM} CO2 Removal System

conditions were analyzed, as is standard practice. The team used a rigorous methodology, including additional LOPA-style methodology. How-

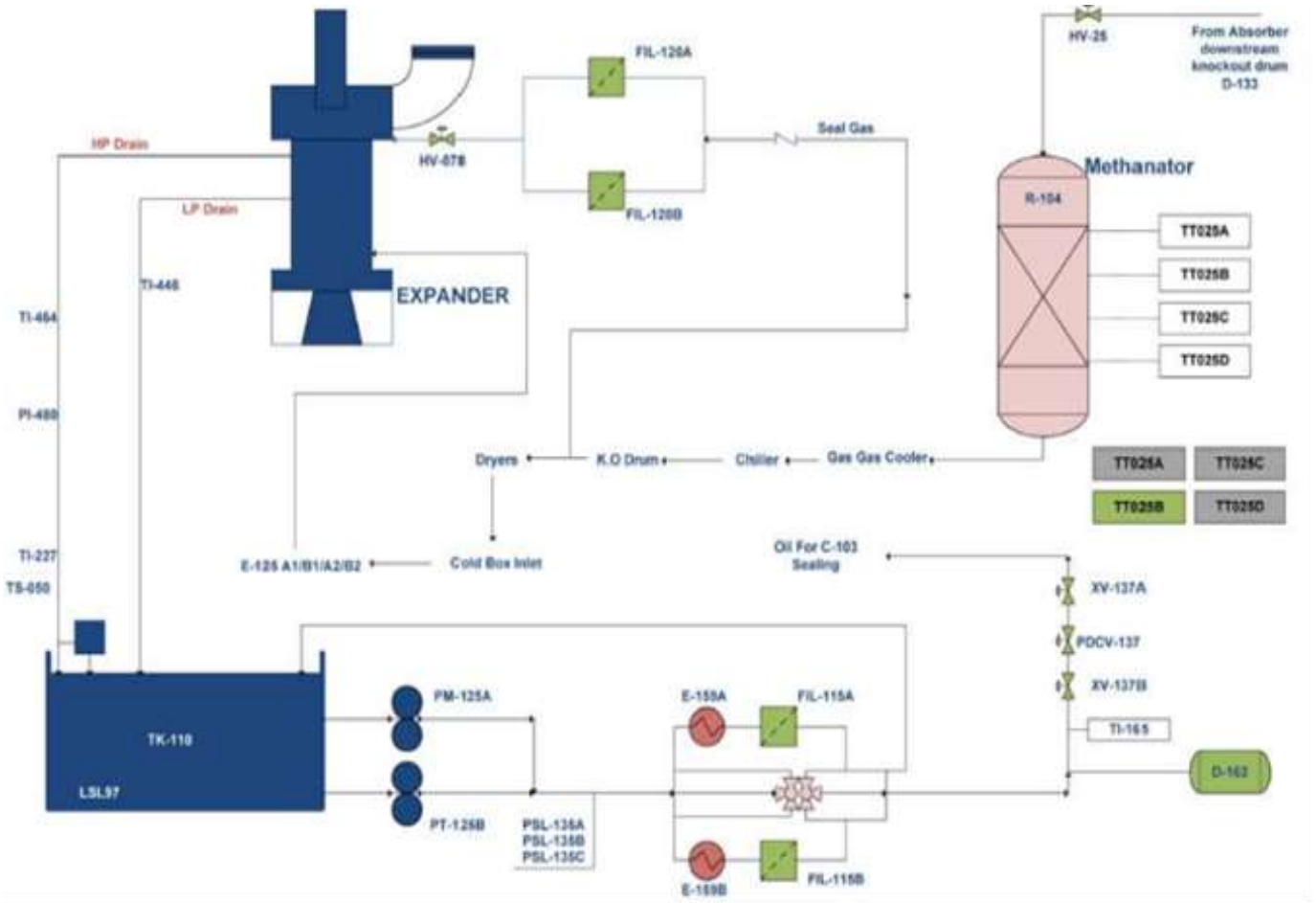

Figure 2: Methanator selector Switches and discontinuation of seal gas flow

HAZOP Summary:

The HAZOP study was performed following industry standard recommended practices, and was led by HAZOP facilitators with decades of expert professional HAZOP experience. The HAZOP team was a multi-disciplinary team that was experienced and fully qualified to perform HAZOP. All HAZOP results were independently reviewed to identify possible gaps or omissions.

The HAZOP did produce useful insights about potential hazards that must be mitigated. Total 436 action were generated with the majority related to interlocks, alarms, control actions and procedural control. “No Flow” and many other

ever, a comparison of the HAZOP results and the actual operating experience, which was not available to the HAZOP team, showed that the HAZOP did not identify the missing requirements of seal gas supply valve cutoff during Methanator tripping that contributed to the hydrogen fire.

The original HAZOP could be updated after the event using hindsight knowledge of the costly new flaws that were discovered during operation. Although that is true, the fact remains that the original team—who did not have the benefit of hindsight knowledge—were unable to catch the flaws involving the interactions between physical

components, digital I&C behaviors, and human interactions.

Once the flaw is understood, Hindsight Bias [22] makes the flaw seem more obvious than it was without hindsight. Hindsight Bias creates overconfidence that that particular flaw should have been caught or that it would have been caught if only we had been on that team. To avoid the bias, we need to rely on empirical data rather than guesses about whether it could have been theoretically identified. We did not evaluate whether HAZOP teams could identify this flaw with hindsight knowledge of the flaw. We evaluated whether qualified teams with no hindsight knowledge of the flaw could reliably and consistently discover these flaws using HAZOP. The fact is that teams of fully qualified professionals did not identify these flaws despite decades of experience in HAZOP, the plant, and the chemical processes involved, despite a rigorous state-of-the-art HAZOP methodology, independent reviews, and an additional LOPA-style methodology.

As discussed earlier, this is not the first flaw that has been missed by HAZOP in the process industries and it will not be the last. The authors decided to perform an empirical comparison between HAZOP and alternative methods when performed by teams with no hindsight knowledge of flaws in the system.

STPA Summary:

With the growing adoption of STPA in the process industries to analyze interactions between physical, digital, and human components [15, 17], the authors selected STPA for an empirical comparison using the same system and qualified STPA practitioners. A limited STPA was applied on the same system without knowing the incident that happened, the root causes, or the necessary corrective actions to address the hidden weaknesses in the system.

STPA is performed in four steps: [23]

1. Define the purpose of the analysis, including the losses to prevent. Note that STPA is not limited to explosions or loss of life. STPA can be used to prevent other losses such as loss of production.
2. Model the control structure, which identifies the feedback control loops.
3. Identify Unsafe Control Actions (UCAs) that will lead to a hazard.
4. Identify scenarios that explain why those unsafe behaviors and decisions would occur.

Defining the purpose of the analysis is the first step. What kinds of losses will the analysis aim to prevent? Will STPA be applied only to traditional safety goals like preventing loss of human life or will it be applied more broadly to security, privacy, performance, and other system properties? What is the system to be analyzed and what is the system boundary? These and other
Fundamental questions are addressed during this step.

The second step is to build a model of the system called a control structure. A control structure captures functional relationships and interactions by modeling the system as a set of feedback control loops. The control structure usually begins at a very abstract level and is iteratively refined to capture more detail about the system.

The third step is to analyze control actions in the control structure to examine how they could lead to the losses defined in the first step. These unsafe control actions are used to create functional requirements and constraints for the system.
The fourth step identifies the reasons why unsafe control might occur in the system. Scenarios are created to explain:

a) How incorrect feedback, inadequate requirements, design errors, parameter deviations, component failures, and other factors could cause unsafe control actions and ultimately lead to losses.
b) How safe control actions might be provided but not followed or executed properly, leading to a loss.

Once scenarios are identified, they can be used to create additional requirements, identify mitigations, drive the architecture, make design recommendations and new design decisions (if STPA is used during development), evaluate/revisit existing design decisions and identify gaps (if STPA is used after the design is finished), define test cases and create test plans, develop leading indicators of risk, and for other uses as described the STPA handbook.

The following summarizes a portion of the STPA results.

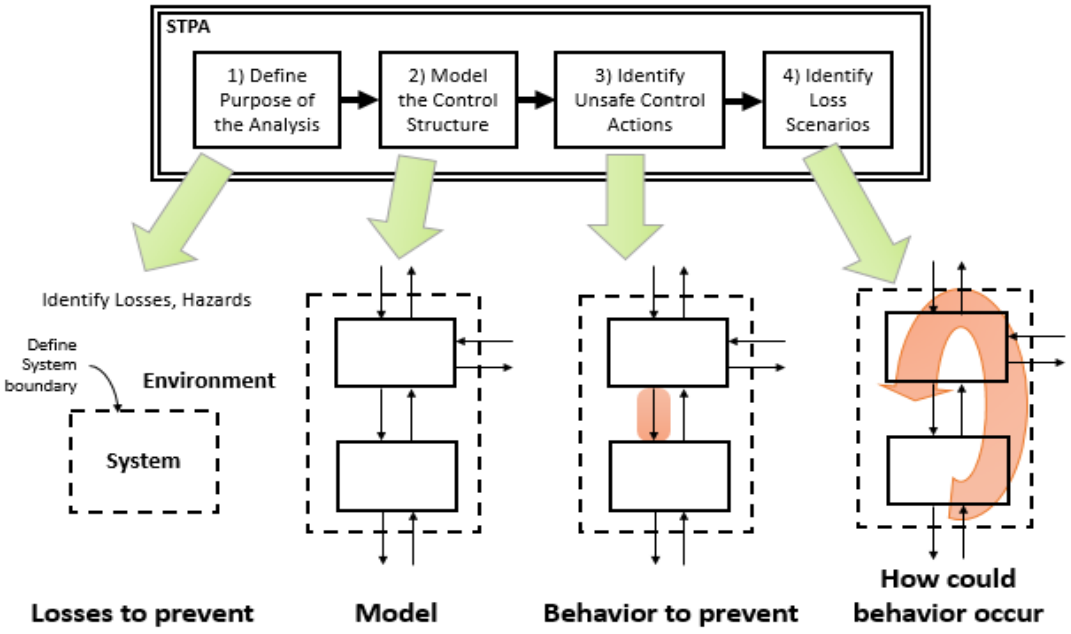

Figure 3: The four steps of STPA from the STPA Handbook

STPA identified the following losses:
L1: Loss of life or injury
L2: Equipment damage
L3: Environmental contamination
L4: Loss of production

Next, STPA identifies high-level system hazards. A system hazard is an overall system state that will lead to losses in a worst-case environment. STPA identified the following hazards for the overall Ammonia Plant Production (APP):
SH-1: APP physically injures people (rupture, fire, etc.) [L1,L2,L3,L4]
SH-2: APP equipment is operated beyond limits [L1,L2,L3,L4]
SH-3: APP releases toxic chemicals into the environment [L3,L4]
SH-4: APP unable to produce sufficient product or high-quality product [L4]

The second step of STPA is to model the control structure. The control structure identifies the controls that oversee and supervise the physical controlled processes—including human, automated, and other controllers—as well as the specific control actions (downward arrows) that can be used to execute control over the controlled processes. The control structure also identified feedback information (upward arrows) that can be used by controllers to inform decision-making and select appropriate control actions. Figure 4 shows an example of a simplified control structure for this application**.**

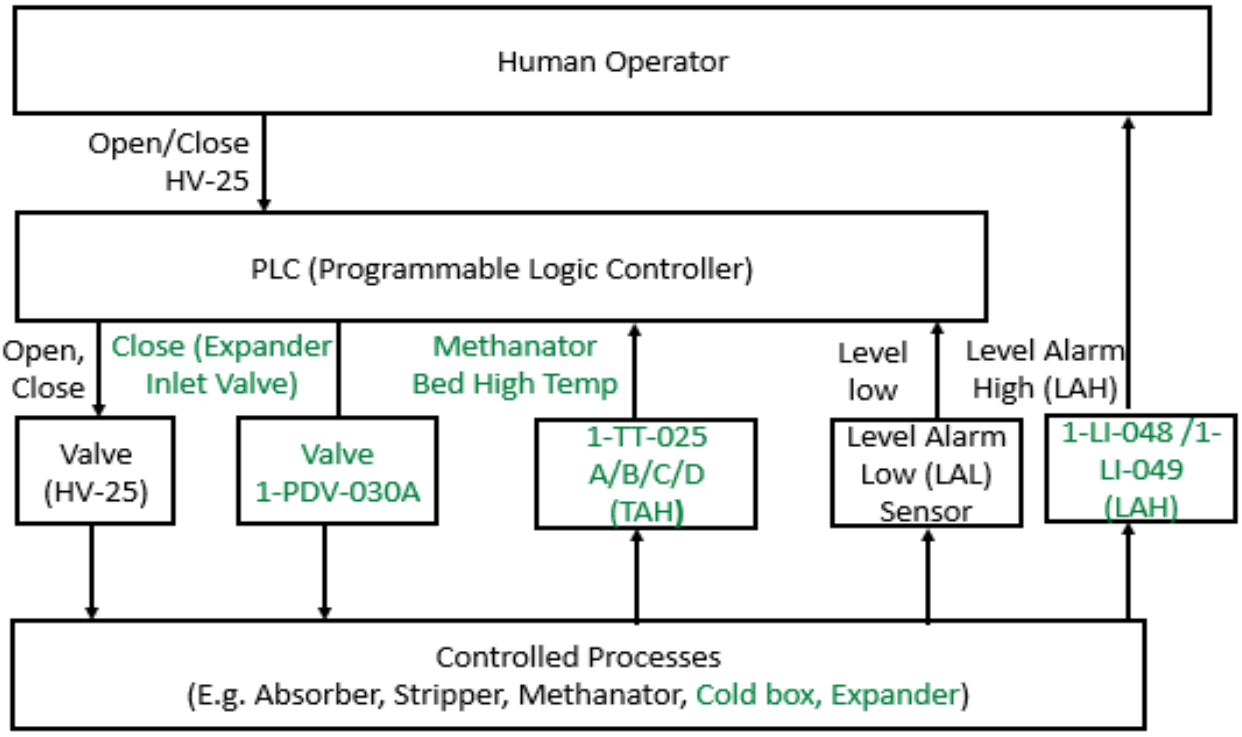

Figure 4: Example of a Simplified Control Structure

The third step of STPA identifies control actions that are unsafe. These Unsafe Control Actions (UCAs) specify a control action as well as a context in which that control action is unsafe, meaning it is a cause of one or more system hazards in the first step. UCAs are identified for all controllers in the control structure, including both automated and human controllers. No assumption is made that the automation is designed correctly or that human procedures exist and are specified correctly. In other words, UCAs are do not identify deviations from a specified requirement or design intent that is assumed to be perfect. UCAs may describe behavior that is required, that is not required, that is intended, or that is not intended.

For example, "UCA-1: PLC does not provide Close HV-25 Command when actual liquid level is high in the Absorber" is unsafe because leaving HV-25 open when liquid level is high will lead to entrainment of Catacarb solution. UCA-1 does not assume that a requirement or a design intent already exists for the PLC to provide the Close HV-25 Command in this condition. The UCAs can be compared to the design intent and the requirements in a later step to identify missing, incomplete, incorrect, conflicting, or unsafe requirements, assumptions, and design intentions.

Tables 2 and 3 identify additional UCAs for both the automated and human controllers in Figure 4.

Table 2: STPA Unsafe Control Actions for the PLC

Source Controller: PLC				
Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Close HV-25 Cmd	UCA-1: PLC does not provide Close HV-25 Cmd when actual liquid level is high in the Absorber. [SH-2, SH-3, SH-4]	UCA-2: PLC provides Close HV-25 Cmd when actual liquid level is absorber is normal (cause Methanator trip). [SH-4] UCA-3: PLC provides Close HV-25 Cmd while expander remains in service (causes low seal gas flow to expander which will eventually result in fire) [SH-1,SH-2,SH-4]	UCA-4: PLC provides Close HV-25 Cmd too early when liquid level is high (trip set point) [SH-4] UCA 5: PLC provides Close HV-25 Cmd too late when liquid level in absorber is high (causes solution carryover to Methanator causing run away of reaction which will lead to Methanator vessel failure) SH-1,SH-2,SH-4]	UCA-6: PLC continues providing Close HV-25 Cmd too long after liquid level is normal (will prevent startup when issue is resolved) UCA-7: PLC stops providing Close HV-25 Cmd too soon before valve has fully closed UCA-8: PLC stops providing Close HV-25 Cmd too soon before liquid level in absorber has returned to normal
Open HV-25 Cmd	NA	NA	NA	NA

Table 3: STPA Unsafe Control Actions for the Human Operator

Source Controller: Operator				
Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Close HV-25 Cmd	UCA-9: Operator does not provide Close HV-25 Cmd when actual liquid level is high in the Absorber (due to malfunctioning of level indicator or excessive foaming) [SH-2, SH-3, SH-4]	UCA-10: Operator provides Close HV-25 Cmd when actual liquid level is absorber is normal (cause Methanator trip). [SH-4] UCA-11: Operator provides Close HV-25 Cmd while expander remains in service (causes low seal gas flow to expander which will eventually result in fire) [SH-1,SH-2,SH-4]	UCA-12: Operator provides Close HV-25 Cmd too early when liquid level is high (trip set point) [SH-4] UCA 13: Operator provides Close HV-25 Cmd too late when liquid level in absorber is high (causes solution carryover to Methanator causing run away of reaction which will lead to Methanator vessel failure) SH-1,SH-2,SH-4]	UCA-14: Operator continues providing Close HV-25 Cmd too long after liquid level is normal (will prevent startup when issue is resolved) UCA-15: Operator stops providing Close HV-25 Cmd too soon before valve has fully closed UCA-16: Operator stops providing Close HV-25 Cmd too soon before liquid level in absorber has returned to normal
Open HV-25 Cmd	UCA-17: Operator does not provide Open HV-25 Cmd during startup [SH-3, SH-4]	UCA-18: Operator provides Open HV-25 Cmd when liquid level is high [SH-2, SH-4]	UCA 19: Operator provides Open HV-25 Cmd too soon during startup (causes quick pressurization of Methanator will result leakage, catalyst damage etc.)[SH-1, SH-2, SH-3, SH-4] UCA 20: Operator provides Open HV-25 too late during startup [SH-2, SH-4] UCA 22: Operator provide Open HV-25 Cmd too soon during startup which cause high CO2 slippage enter Methanator and will cause temperature run away. [SH-1, SH-2, SH-3, SH-4]	UCA-21: Operator continues providing Open HV-25 Cmd too long when liquid level is high [SH-2, SH-4] UCA-22: Operator stops providing Open HV-25 Cmd too soon before vent is completely shifted downstream during startup

Once the UCAs are identified, STPA can generate PLC requirements and human procedures that are necessary to prevent the UCAs. For example, these two requirements were generated by STPA:

R-1.1: PLC shall be designed to provide Close HV-25 Command when actual liquid level is above X in the absorber [UCA-1]

R-1.2: PLC shall be designed to receive feedback that indicates when actual liquid level is above X in the absorber [UCA-1]

The fourth step of STPA is to build scenarios that explain why unsafe decisions and unsafe behaviors will occur in the system. The STPA Handbook contains detailed guidance about the types of scenarios that can be constructed and how to construct them.

The following two scenarios were among those identified by STPA.

UCA-3: PLC provides Close HV-25 Command while expander remains in service *(causes low seal gas flow to expander which will eventually result in fire)* [SH-1, SH-2, SH-4]

Why? PLC Control Algorithm #1: The PLC control algorithm has no logic or design intent to trip the expander in case of low seal gas pressure/flow as a result of HV-25 closure. This condition is missing from the requirements and the PLC logic.

Solution: Add requirement R-CA.1: DCS logic shall provide automatic Expander Trip Command when HV-25 is closed.

UCA-23: Operator does not manually trip Expander C-103 when HV-25 is closed *(causes low seal gas flow to expander which will eventually result in fire)* [SH-1, SH-2, SH-4]

Following are some possible reasons that can lead to inappropriate actions:

Why? Human Decision-making #1: The operator has no training or operational procedure to trip the expander in case of HV-25 closure. (Missing procedure, inadequate training for this procedure, conflicts with experience, etc.)

Why? Human Belief #1: The operator believes (correctly) that downstream alarms require attention, causing the operator to forget to trip the expander

Why? Human Belief #2: The operator believes (incorrectly) that the expander is already tripped automatically and does not need to be manually tripped

Why? Human Feedback #1: The HMI design has no alert or warning to indicate that HV-25 is closed without an expander trip (fire danger).

Why? Human Feedback #2: The RPM (Revolutions per minute) signal is not visible to the operator on DCS by design, so the operator is not able to determine the hazardous state of the system

Why? Human Feedback #3: The operator receives incorrect pressure reading for seal gas

Solutions:

- Add an alert or warning to indicate when a fire danger exists due to HV-25 closed without an expander trip.
- Automatic tripping of expander in case of I-006 (Methanator trip logic) actuation

Comparison Results and Discussion

Both HAZOP and STPA produced useful insights about potential causes of hazards and losses. Common results related to physical behaviors, failures, and deviations in the controlled processes were identified by both methods, such as a valve blockage or failure. The most significant difference is that the HAZOP results—performed by expert practitioners and

with comprehensive reviews—did not adequately consider:

- Weaknesses in the intended design of the automation
- Missing logic or unsafe logic in automated controllers
- Safety-critical functionality missing from the design
- Missing feedback information to enable safe decision-making by controllers
- Interactions between multiple controllers
- Incorrect operational assumptions made by human operators, especially assumptions about the automation
- Inconsistent automation that will cause human operator confusion, like automatic mode changes or an automatic trip function that works in almost every possible case except one
- Gaps in human procedures or training
- Assumptions about human operator behaviors that were not validated
- Potentially conflicting commands from multiple controllers, such as a condition that simultaneously triggers an automated downstream trip and a manual human command to open a valve
- Common causes that defeat assumptions about redundancy and independence

STPA produced new scenarios not found by HAZOP that considered both human and automated decision-making, including decisions and beliefs that may appear reasonable at the time given the information available and other contextual factors.

STPA produced safety-critical requirements and recommendations that were missed by HAZOP, including effective low-cost solutions. In this study STPA was applied after the design was created and implemented, but most of the STPA results could have been obtained much earlier in the development process before flawed logic and flawed procedures were implemented.

The HAZOP and STPA results were compared to real operational incidents and losses that were unknown to the teams when the analysis was performed. None of the causes of the real incidents were found in the HAZOP results, although that is not too surprising because a full HAZOP was already performed on the system before it went into operation as a standard practice. The HAZOP results missed all of the safety-critical weaknesses and corrective actions that were discovered after the system was put into operation.

The STPA scenarios included the actual scenarios that caused losses in operation, especially the human and automation behaviors that were not foreseen by the original developers. The STPA results, which were produced from a general system description with no knowledge of the actual weaknesses and operational incidents, matched the corrective actions from the real incidents that were within the scope of the STPA effort. The STPA effort also produced additional corrective actions that were not found in the root cause analysis but would have prevented the incidents.

Limitations

This study was subject to a number of limitations. The STPA team was less than half the size of the HAZOP team. The time allocated to perform STPA was less than half that of HAZOP. The HAZOP team consisted of many domain experts who were fluent in the detailed design and operation of the system, while the STPA team had less familiarity with the system. The STPA team did have the ability to ask specific questions about the system if the questions were generated by the analysis. All information and answers were limited to materials available before the operation of the system and the incidents that occurred.

Conclusion

Although the popular HAZOP method was shown to provide useful insights, the HAZOP method is not perfect even when performed by

expert practitioners with multiple reviews and in compliance with industry standards. HAZOP was found to overlook important causes related to new technology, human behavior, and interactions between non-failed components operated as designed. The STPA method was found to address the gaps that were empirically observed in the HAZOP method, including identification of real scenarios and real corrective actions that otherwise were not discovered by HAZOP until hazardous and costly losses occurred during operation.

References

[1] Process Safety Culture Toolkit Building process safety culture; tools to enhance process safety performance (ISBN # 0-8169-0999-7)

[2] Process Safety Beacon Dec 2009 CCPS

[3] "Phillips Petroleum Chemical Plant Explosion and Fire", U.S. Fire Administration/Technical Report Series, USFA-TR-035/October 1989

[4] The Washington Post, July 19, 1990, (Jan, 31, 2022) Blast in Cincinnati kills at least 1, Injuries dozen, https://www.washingtonpost.com/archive/politics/1990/07/20/blast-in-cincinnati-kills-at-least-1-injures-dozens/f450fab9-2f12-48b4-a165-6861598136b7/

[5] UPI Archives, May 13, 1991, (Jan, 31, 2022) Cause of fatal fertilizer plant explosion still unknown, https://www.upi.com/Archives/1991/05/13/Cause-of-fatal-fertilizer-plant-explosion-still-unknown/2805674107200/

[6] "Investigation Report Refinery Explosion and fire", U.S. Chemical Safety and Hazard Investigation Board, Report No 2005-04-I-TX, March 2007

[7] Process Safety Beacon, Aug 2010

[8] Ammonia Technical Manual 1976: Ammonia loading line rupture

[9] IEC 61882: Hazard and operability studies (HAZOP studies) Application guide

[10] Simon Schubach, A modified computer hazard and operability study procedure, Journal of Loss Prevention in the Process Industries, Volume 10, Issues 5–6, 1997, Pages 303-307, ISSN 0950-4230

[11] R. Kennedy, B. Kirwan, Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high risk systems, Safety Science, Volume 30, Issue 3, 1998, Pages 249-274, ISSN 0925-7535,

[12] Kirwan, B. and L.K. Ainsworth. (1992). A Guide to task analysis, Taylor & Francis, London.

[13] D. J. Burns and R. M. Pitblado, "A modified HAZOP methodology for safety critical system assessment", in Directions in Safety-critical Systems: Proceedings of the Safety-critical Systems Symposium, Bristol 1993, F. Redmill and T. Anderson, Eds. Feb. 1993, pp. 232–245, Springer-Verlag.

[14] A New Accident Model for Engineering Safer Systems", Nancy Leveson, Safety Science, 2004

Engineering a Safer World", MIT Press, Nancy Leveson, 2012

[15] NRC & NEI "Guidance for Addressing CCF in High Safety Significant Safety-related DI&C Systems", ML21173A286, 2021

NuScale "NuScale Standard Plant Design Certification Application", chapter 7 "instrumentation and controls", December 2016 https://www.nrc.gov/docs/ML1701/ML17013A278.pdf

NuScale "Use of STPA in the Development of a Reactor Protection System at NuScale Power" MIT STAMP Workshop, 2020

EPRI, Hazard Analysis Demonstration – Generator Exciter Replacement: Lessons Learned, EPRI 3002006956, 2015

U.S. NUCLEAR REGULATORY COMMISSION STANDARD REVIEW PLAN, BRANCH TECHNICAL POSITION 7-19, August 2020

M. Gibson, “Integration of STPA into EPRI Risk-Informed Digital Engineering Framework”, 2020 MIT STAMP Workshop

[16] STATEMENT BY Ms. STACY CUMMINGS
BEFORE THE UNITED STATES SENATE COMMITTEE ON ARMED SERVICES ON DEFENSE ACQUISITION PROGRAMS AND ACQUISITION REFORM
https://www.armed-services.senate.gov/imo/media/doc/USD%20(PTDO)%20Cummings%20-%20Written%20Testimony_SASC%20Hearing%2028%20APRIL%202021.pdf

[17] Esteban Montero, Application of STPA to understand marine operations at Chevron, MIT STAMP Workshop, 2017

M. Rodriguez, I. Diaz, “STPA: A SYSTEMIC AND INTEGRAL HAZARDS ANALYSIS TECHNIQUE APPLIED TO THE PROCESS INDUSTRY”, AIChE Spring Meeting and Global Congress on Process Safety, 2015, AiChE Academy

Leveson & Stephanopolous, A system-theoretic, control-inspired view and approach to process safety, AiChE Journal, 2013

J.J. Horng, Analysis of Shell Moerdijk Accident by Systems-Theoretic Accident Model and Processes and Bowtie Analysis, 2019, AIChE Spring Meeting and Global Congress on Process Safety

K. Forde, T. Stirrup, Introduction to STPA Hazard Evaluation Technique: A New Tool in Theih/OS Tool Box, 2018, AIChE Spring Meeting and Global Congress on Process Safety

[18] U.S. DOT/FAA “Software Assurance Approaches, Considerations, and Limitations: Final Report”, TC-15/57, 2016

Andrea Scarinci, Felipe Oliveira, Amanda Quilici , Danilo Ribeiro , Ricardo Moraes , Daniel Pereira , “STPA application Air Management System Commercial Aviation”, MIT STAMP Workshop, 2017

Ricardo Moraes, ASTM Standard Guide for Application of STPA to Aircraft, MIT STAMP Workshop, 2020

Montes, Dan, STPA use in the U.S. Air Force, MIT STAMP Workshop 2020

Scott Reeves, STAMP at FedEx Air Operations, MIT STAMP Workshop 2020

Gus Larard, Importance of Organizational Culture in Effective Safety Management, MIT STAMP Workshop 2020

Blake Abrecht, Dave Arterburn, David Horney, Jonathan Schneider, “A New Approach to Hazard Analysis for Rotorcraft”, American Helicopter Society 2016

[19] Rodrigo Sotomayor, 2015, “Comparing STPA and FMEA on an Automotive Electric Power Steering System”

Hossam Yahia & Esmaiel Fawzy, “STAMP/STPA case study: Range Extender System for Electric Vehicles”, MIT STAMP Workshop, 2013

ISO/PAS 21448: 2019 Road Vehicles – Safety of the Intended Functionality, Automotive Safety Standard

SAE J3187 “System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems”

[20] Ammonia Technical Manual

[21] Ammonia Technical Manual 2015: Foaming of Catacarb™ CO2 Removal System leads to Methanator Runaway Reaction and Expander Fire Incident (abridged)

[22] Neal J. Roese1 and Kathleen D.Vohs, “Hindsight Bias”, Perspectives on Psychological Science, 2018, 7(5) 411–426

[23] STPA Handbook Nancy G. Leveson and John P. Thomas