CHEMICAL ENGINEERING TRANSACTIONS

VOL. 90, 2022

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Aleš Bernatík, Bruno Fabiano
Copyright © 2022, AIDIC Servizi S.r.l.
ISBN 978-88-95608-88-4; **ISSN** 2283-9216

DOI: 10.3303/CET2290044

A Systemic Approach Methodology to Measure Process and Plant Safety

Manuel Rodriguez Hernandez*, Abouzar Yousefi
Chemical and Environmental Engineering, Universidad Politecnica de Madrid, Spain
manuel.rodriguezh@upm.es

Major accidents continue to happen in the process industry and often have serious consequences. There are questions on how these accidents happen and how we can monitor safety in a process plant to prevent these accidents from happening. The possibility of measuring the safety level in a process plant is very compelling and different approaches using key performing indicators (leading and lagging indicators with some metrics) have been proposed. The industry has evolved towards a complex sociotechnical environment where the traditional accident causation models used that try to explain how and why accidents happen are no longer valid (or at least are not the fittest option) to analyse these complex systems. New accident models have been developed lately trying to cope with the complexity of new industrial systems. These (relatively) new systemic models have their roots in systems theory. In this work, a novel methodology is presented to measure safety level in a process plant using a systemic approach. The systemic model used in this work is Systems Theoretic Accident Model and Processes (STAMP). The measurement of the safety level is done according to the status of safety checkpoints which is a new concept introduced in this work. A safety checkpoint is a requirement defined to prevent a loss scenario to happen or to satisfy safety measures associated to the loss scenario. The outcome of the analysis obtained with this methodology can be presented in different ways to help management to make informed risk-based decisions and take the actions needed to prevent accidents.

1. Introduction

There are different regulations in different countries regarding the process industry, all of them have a common objective and it is the prevention and control of major accidents. In this regard, companies in the process industry spend resources to prevent accidents from happening. Different studies and activities are usually carried out at different times to prevent accidents or mitigate their consequences like Hazard Identification (HAZID), BowTie Analysis, Hazard and Operability Studies (HAZOP), Safety Integrity Level (SIL) Study, etc. These studies are done by companies during the design, construction, commissioning, start up and operation in order to establish and maintain safety requirements for accident prevention and mitigation. Despite these efforts, major accidents continue to occur in the process industry and often have serious consequences. These accidents have raised concerns with the public, stakeholders, and regulators (OECD, 2012). One of the main reasons is that most of the techniques commonly used are based on accident causation models that were developed many years ago. There is an argument that significant changes have occurred in the process industry (Leveson 2012), but safety study and accident prevention have not been updated accordingly. Consequently, these traditional techniques may have limitations in identifying hazards related to the modern process industry.

System based accident models or systemic accident models have been introduced recently to deal with the complexity of the systems. Systemic models view accidents as emergent phenomena that arise from interactions among system components, where the interactions may be non-linear and involve multiple feedback loops (Perrow, 1984).

One of the systemic models is STAMP (Systems-Theoretic Accident Model and Processes) introduced by Leveson (2004). STAMP defines the whole sociotechnical system and the control structure associated to it. The information goes from the lower levels of the structure (physical equipment) to the top levels (company management and regulatory bodies) and the actions the other way around (from top to bottom). All the

Paper Received: 7 January 2022; Revised: 14 March 2022; Accepted: 7 May 2022
Please cite this article as: Rodriguez Hernandez M., Yousefi A., 2022, A systemic approach methodology to measure process and plant safety, Chemical Engineering Transactions, 90, 259-264 DOI:10.3303/CET2290044

components in the structure are interrelated and accidents/incidents can arise not only from failures of individual components but from not considered or unintended interactions between components. This view considers safety as a control problem and thus the methodology tries to impose measures and enforce constraints to avoid the loss of control that would lead to an accident. STAMP has two main techniques one devoted to safety analysis, STPA (System Theoretic Process Analysis) and the other one CAST (Causal Analysis using System Theory) devoted to accident analysis. STPA will be briefly explained as it is the basis of the methodology devised to measure process safety.

1.1 STPA

STPA works on a model (the control structure) of the system under analysis. As previously indicated the model is a functional control diagram and the analysis focus on how control is achieved and on what can go wrong in every component of the control structure. The STPA procedure is developed through the following steps:

Step 1: Define the purpose of the analysis. In this stage the system boundary is specified as well as the possible losses and hazards in the system. System-level safety constraints are also defined in this initial step.

Step 2: Model the control structure. The control structure of the system is drawn, the process model is created and its variables identified.

Step 3: Identify unsafe control actions (UCAs). First, control actions are identified, and then, different behaviours of these actions are postulated. The possible behaviours are: control action provided, not provided, provided too early or too late or stopped too soon. Behaviours leading to unsafe control actions are determined and the constraints needed to avoid them specified.

Step 4: Identify loss scenarios. The possible loss scenarios derived from the unsafe control actions are identified as well as the recommendations to mitigate or eliminate the associated hazards.

In this paper, a methodology is developed extending the STPA technique to monitor and measure the safety level of process plants. The methodology is explained in section 2. Then, it is applied to a process plant and the outcome is provided in section 3. Finally, conclusions are presented in the last section.

2. Methodology

Traditionally safety has been defined related to (the absence of) accidents and incidents (Rasmussen and Svedung, 2000) or (IEC/ISO, 1999). This approach, focus on unsafety more than on safety, the process safety management is driven by measurements related to the absence of safety (like the number of days without injuries for example) more than by measurements related to the presence of safety (Hollnagel, 2012). This leads the existing methodologies based on safety indicators that measure accidents, incidents or near misses. Recently, Hollnagel (2014), proposed an approach that addressed safety when things go right (defined it as Safety-II), basically looking at what happens when safety is present (the plant is successfully operating). The methodology presented in this work aligns with the Safety-II concept and utilizes STPA as the underlying technique to measure the safety status of a plant (when things are operating normally). Previous approaches exist like Knegtering and Pasman (2013) that used various safety indicators to measure the safety level using bow-ties or like Marono et al. (2006) who introduced a operational safety index (called ‘PROCESO’) for safety self-assessment in chemical and petrochemical plants, their methodology relied mainly on expert judgement (on the identified safety areas that composed the safety index). The methodology presented here has two differential characteristics: it is based on a systemic model and uses a new concept called ‘safety checkpoint’ that is added to STPA and allows to derive a measure of the safety of the plant. Safety checkpoints are defined for loss scenarios and safety recommendations, they assess how well loss scenarios are under control and how safety recommendations are implemented, in the sense of the already mentioned Safety-II view. With this approach, all the system is studied as a whole, and all the loss scenarios are identified. Then, loss scenarios and their controls are monitored via safety checkpoints that literally means measuring the safety status of the system as a whole.

The first four steps are as explained when introducing STPA in the previous section. These steps are completed with the following ones:

Step 5. Checkpoints definition: Define safety checkpoint for each loss scenario/safety measure. It includes definition of data source for each safety checkpoint, the frequency of obtaining the data and expected data for each safety checkpoint.

Step 6. Checkpoints consolidation. Once identified, they are analysed and consolidated (eliminating repetitions and combining related ones) and a final list is produced. At this point, a weight is assigned to each safety checkpoint taking into account the number of loss scenarios related to each one.

Step 7. Evaluate plant safety level. On every checkpoint, the indicator, acceptability criteria and level of safety is defined. Using this safety level and the weight, a cumulative safety level is calculated that represent the overall safety status of the plant.

3. Case study: application to a process plant

3.1 Process description

The presented methodology is applied to a section of a process plant in a gas production facility. The site comprises the production wells, a gathering system and the process plant with its coolers, separators and compressors. A train air cooler and a separator are the plant section included in this work. The stream, from the well, is fed to the air cooler at 250-280ºF and 870psig. The exchanger decreases the temperature to 120ºF. The control temperature of the cooler is achieved using a motor speed controller that manipulates the speed of the fans. The outlet temperature of the air coolers influences the facility performance as a lower outlet temperature improves plant efficiency. The outlet of the air cooler is fed to the separator where three different phases are separated: gas, organic phase (hydrocarbon) and water. To control the liquid inventories in the separator two control level loops exist. One of them controls the liquid-liquid interface and the other one the hydrocarbon condensate level. The water is sent to the produced water tanks and the hydrocarbon to the stabilizer. There is one emergency shutdown valve (ESDV) before the air cooler, this valve closes if the level increases above a high-high level limit established. If the hydrocarbon condensate level decreases below a low level trip point then the outlet control valve closes, a similar procedure is implemented for low level water.

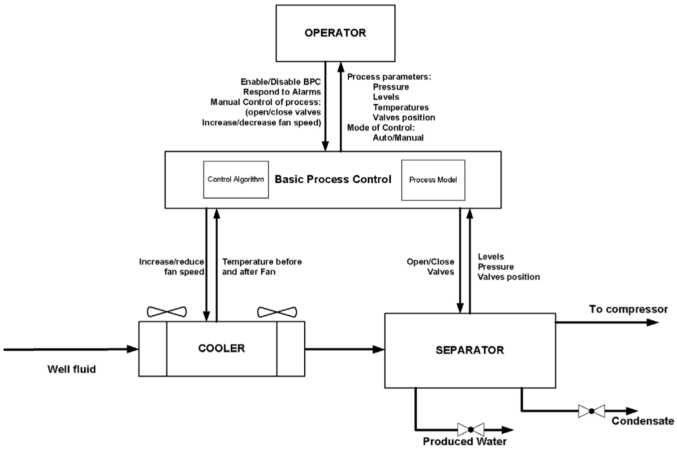

Figure 1: Process under analysis and its detailed Control Structure

Figure 1 shows the system under study and the information flow between the lower layers of the sociotechnical system: physical equipment, basic process control and operations. This will be used as the control structure to perform the safety analysis.

3.2 Safety analysis

The boundaries for this case study are set by the air cooler and the separator (including their incoming and outgoing streams). The losses identified are: L-1: Loss of human life or injury to people, L-2: Environmental loss, L-3: Loss of or damage to asset

The hazards identified are: H-1: Uncontrolled or unplanned release of hydrocarbon ignited (related to L-1, l-3), H-2: Uncontrolled or unplanned release of liquid hydrocarbon reaching the environment (related to L-2)

Step 2. Model the control structure. This is the one presented in Figure 1.

Step 3. Identify unsafe control actions (UCAs).

Some of the identified unsafe control actions are defined in Table 1.

Table 1: Identified Unsafe Control Actions from the refined control structure

Control Action	Not providing	Providing	Too early, too late, out of order	Stopped too soon, applied too long
BPC Opens Produced water valve	BPC does not provide Open valve function when water level is high in the separator, causing water enter to the condensate stream. N/A	UCA-1: BPC provide Open produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]		UCA-2: BPC maintain Open produced water valve function for too long causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]
BPC Closes Produced water valve	UCA-3: BPC does not provide Close produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	BPC provide Close valve function when water level is high in the separator, causing water enter to the condensate stream. N/A	UCA-4: BPC provides Close produced water valve function too late while water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	

Step 4. Identify loss scenarios associated to the UCAs.
Considering the identified UCAs, loss scenarios are identified. An example of the identified loss scenarios for UCA-1 are presented in table 2.

Table 2: Identified loss scenarios for Unsafe Control Actions

Unsafe Control Actions	Loss Scenarios
UCA-1: Automated process control does not provide the BPC function when the process is out of normal conditions [H1, H2]	Scenario 1 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are not capable to detect the abnormal conditions (not the right sensors selected) [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are faulty due inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]

After the loss scenarios have been identified recommendations are issued, table 3 show the defined recommendations for Scenario 1 for UCA-1.

Table 3: Recommendations defined for identified loss scenarios related to generic control structure

Loss Scenarios	Safety Measures
Scenario 1 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are not capable to detect the abnormal conditions (not the right sensors selected) [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Scenario 1 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are not capable to detect the abnormal conditions (not the right sensors selected) [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]

Step 5. Checkpoints definition

Safety checkpoints are indicators that demonstrate the status of the controls established for each loss scenarios/recommendation. For each loss scenario/recommendation identified safety checkpoints are defined.

Step 6. Checkpoints consolidation.

Initially the safety checkpoints are generated for the high level control structure of the gas facility. The methodology can be used at different levels of abstraction. It can be applied at higher level of the system or at detailed level. In order to have more detailed loss scenarios/recommendations and consequently more detailed safety checkpoints it is necessary to develop a refined control structure. In table 4 an example of on e of the identified checkpoints with the number of related loss scenarios and their weights is presented. The higher the number of loss scenarios monitored by a safety checkpoint the higher the importance of that safety checkpoint in the safety of the plant. In order to define the safety level of the plant it is necessary to define a weighing system for the safety checkpoints. It is understood that different scenarios could have different likelihoods to happen and could result in different consequences. However, in this case to simplify the study and since all scenarios are related to both hazards (H1 a H2), the number of loss scenarios related to each safety checkpoint is considered as the weighing system.

Table 4: Number of loss scenarios and weighing related to consolidated safety checkpoints

	Safety Checkpoint	Number of related loss scenarios	Weighing (%)
1	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	3	2.5%

Step 7. Evaluate plant safety level

The indicator, acceptability criteria and safety level for each safety checkpoint are defined, as illustrated in table 5 for the previous checkpoint. These are established by experts from the process plant based on the Company policy and international best practices.

The formula described in Equation 1 is used to calculate the cumulative safety level of the plant. It is based on the safety level value determined for each safety checkpoint and the weight of that safety checkpoint. To compute the safety level for this case, data has been obtained from the plant under study and the safety level of each safety checkpoint has been determined.

$$\begin{aligned} &\mathit{Cumulative\ Safety\ Level} \\ &\qquad = \sum_{i=1}^{n} \mathit{Safety\ Level\ determined\ for\ Safety\ Checkpoint}\ (i) \\ &\qquad * \mathit{Weight\ of\ the\ Safety\ Checkpoint}\ (i) \end{aligned} \tag{1}$$

Table 5: Indicator, acceptability criteria and safety levels for each safety checkpoint

	Safety Checkpoint	Weight (%)	Indicator	Acceptability criteria / Safety Level		
				0-50	50-85	85-100
1	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	2.5%	Functioning of condensate valve	Condensate valve opens/closes when condensate level is low/high respectively	N/A	Condensate valve does not open/close when condensate level is low/high respectively

Using the indicated equation and the values and weights of each safety checkpoint the cumulative safety level is calculated giving a result of 67,6% which is shown in a gauge (Fig. 2). In addition, the output of this study can be provided in a table that shows the status of every safety checkpoint (under one of the three safety levels defined).

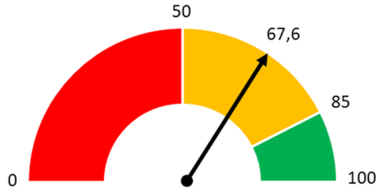

Figure 2: The gauge that shows the safety level of the plant

4. Conclusions

A novel methodology is introduced in this work based on STPA accident model with the purpose of measuring the safety level in process plants and ultimately preventing accidents from happening. The methodology is tested using real data from a process plant with promising results. However, this is only a demonstration to show the capability of the methodology. For industrial use, it is necessary to extend the scope to all the equipment in the plant and higher levels of the sociotechnical structure of the process plant. Safety level can be visualized in a safety gauge format and the status of safety checkpoints could provide additional information to the management in a dashboard. To validate the methodology, it is necessary to use it in a process plant for a period of time long enough for the evaluation and analysis of accident data before and after the implementation of the methodology. It is also required to evaluate the possibility to complete the methodology with quantitative data to have more specific likelihood and consequence information for each loss scenario and consequently more specific weighing system for safety checkpoints.

References

Hollnagel E, 2012, FRAM: the Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems, Farnham, Ashgate

Hollnagel E, Hounsgaard J., Colligan L., 2014, FRAM – the Functional Resonance Analysis Method – a handbook for the practical use of the method, Southern Region of Denmark, Centre for Quality

IEC/ISO, Guide 51: Safety aspects - Guidelines for their inclusion in standards, 1999

Knegtering B., Pasman H, 2013, The safety barometer How safe is my plant today? Is instantaneously measuring safety level utopia or realizable? J. of Loss Prevention in the Process Industries 26, 821-829

Leveson N.G., 2004, A New Accident Model for Engineering Safer Systems, Safety Science, 42, 237-270.

Leveson N.G.,2012, Engineering a Safer Work: Systems Thinking Applied to Safety, The MIT Press, Cambridge, Massachusetts ISBN 978-0-262-01662-9

Marono, M.; Pena, J.A.; Santamarıa, J., 2006, The ‘PROCESO’ index: a new methodology for the evaluation of operational safety in the chemical industry, Reliability Engineering and System Safety, 349-361

OECD, 2012, *Process Safety Guide Corporate governance for process safety: Guidance for senior leaders in high hazard industries. OECD Environment, Health and Safety Chemical Accidents Programme.*

Perrow C., 1984, Normal Accidents: Living with High-Risk Technologies. New York: Basic Books

Rasmussen J., Svedung, I., 2000, Proactive Risk Management in a dynamic society, Karlstad, Swedish Rescue Services Agency