System theory based hazard analysis applied to the process industry

Manuel Rodríguez and Ismael Díaz

1 Introduction

1.1 Chemical process safety: HAZOP is not enough

Industrial chemical processes (refineries, petrochemical, pharmaceutics…) usually work with great amounts of potentially dangerous materials (toxics, explosives, flammables…), very often under extreme conditions (high temperature and/or pressure). That can lead to accidents with the associated human and economic losses. Although safety systems have evolved during the last decades, the reality is that accidents still happen with losses over 1000 million dollar only in USA refineries. The Abnormal Situation Management consortium has shown that losses can be as high as 3–8% of the total plant production (Nimmo, 1995).

The history of process safety is short in comparison with process industry history. Safety regulations have been developed in the last 30 years, usually driven by important accidents (Flixborough in 1974, Seveso in 1976, Three Mile Island in 1979, Bhopal in 1984) causing widespread public concerns about major incidents in chemical plants (Mannan, 2004).

After World War II, the concept of reliability was very closely related to safety. During the last century, some hazard analysis techniques were developed to identify hazards (*chemical, physical or changing conditions that have the potential for causing damage*; Center for Chemical Process Safety, 1999). Those include checklists, what-if analysis, Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). The most widely applied is HAZOP (HAZard and OPerability study), developed by ICI in 1960s. A HAZOP study is a highly disciplined procedure meant to identify how a process may deviate from its design intent. It is defined as the application of a formal, systematic critical examination of the process and the engineering intentions of new or existing facilities to assess the potential for malfunctioning of individual pieces of equipment, and the consequential effects on the facility (Dunjó et al., 2010). It divides the whole system in nodes following Piping & Instrumentation Diagrams (P&IDs). A multidisciplinary team makes the analysis by applying some guidewords to state variables so deviations from design intention are produced and consequence analysis is carried out. One of its main advantages is that it is very intuitive and simple in the application. Besides, the study is systematic and comprehensive, making it very popular for the process industry. So much that an IEC standard (61882:2001) has been developed to homogenise the way of HAZOP application. However, there are some disadvantages in the use of HAZOP as a hazard analysis technique:

- No means to assess hazards involving interactions between different parts of the system.
- No ranking or priorisation of hazards and solutions.
- Time consuming and expensive.
- Both human and organisational factors are rarely taken into consideration and only related to lower levels in the organisational hierarchy.

In addition, from the beginning of using process hazard analysis techniques in the chemical industry, much have been learnt from the accidents occurred that can be summarised as follows (Pasman, 1998):

- The conditions that lead to an accident are often complex and difficult to reproduce.
- Test methods are often inadequate for making reliable predictions.
- A *system approach* appears crucial for successful prevention.

The concurrence of multiple factors in systemic failures is the biggest challenge to cope during the present century. In this way, Hollnagel, Wood and Leveson (2006) proposed *resilience* as the way to deal with complexity. Resilience is seen as *the ability to recover a process from situations that potentially lead to mishap*. Since then, Prof. Nancy Leveson from MIT started working on the systemic approach, resulting in the so-called *System-Theoretic Accident Model and Processes* (STAMP) as detailed in literature (Leveson, 2011).

The shortcomings of the classical accident causation models used in the chemical industry, and why new techniques such as STAMP/STPA are needed, have been deeply discussed by Leveson and Stephanopoulos (2014). They stated that the prevailing assumption of classical models is that accidents are caused by chains of directly related events, what oversimplifies causality. It implies a limitation of the models in that they are unable to go beyond designers' knowledge (it is impossible to find causes that are not considered). Other advantage of STAMP/STPA over classical models is that the latter do not consider many of the systemic factors involved in accidents and the interaction between events as well as the description of the influence of the management-regulation-legislation layer on the process.

1.2 STAMP-STPA foundations

Failures are very rarely caused only by single component or personnel flaws. Traditionally, company management teams tended to consider one person or equipment as the root of accidents, i.e., Union Carbide initially blamed an employee causing Bhopal accident, ignoring other (company) responsibilities such as maintenance, procedures or regulatory agencies. Since 2000, many researchers and company safety teams are claiming a systems engineering point of view of risk management (Rasmussen and Svedung, 2000; Venkatasubramanian, 2011). One of the strongest efforts in order to develop a systemic safety theory has been made by Leveson (2011). She states that safety is an emergent property of the system that is enforced by safety constraints. This is the key assumption of STAMP. Therefore, the goal of STAMP is to control the behaviour of the components and system to ensure that safety constraints are enforced. At each level of the system structure, control loops (Figure 1) exist. In the STAMP model of accident causation, safety is an emergent property that arises when system components interact with each other within a larger environment.

The main advantage of Leveson approach is that its general control loop structure can be applied to all the levels of the socio-technical organisation levels as depicted in Figure 2.

From STAMP general theory, two different techniques have been developed trying to improve, on one hand, existing hazard analysis techniques and, on the other hand, existing accident analysis techniques. These two approaches are STPA (System Theoretic Process Analysis) and CAST (Causal Analysis based on STamp). In this paper we are focused on hazard analysis, so, only the STPA analysis will be taken into account.

Figure 1 General control loop

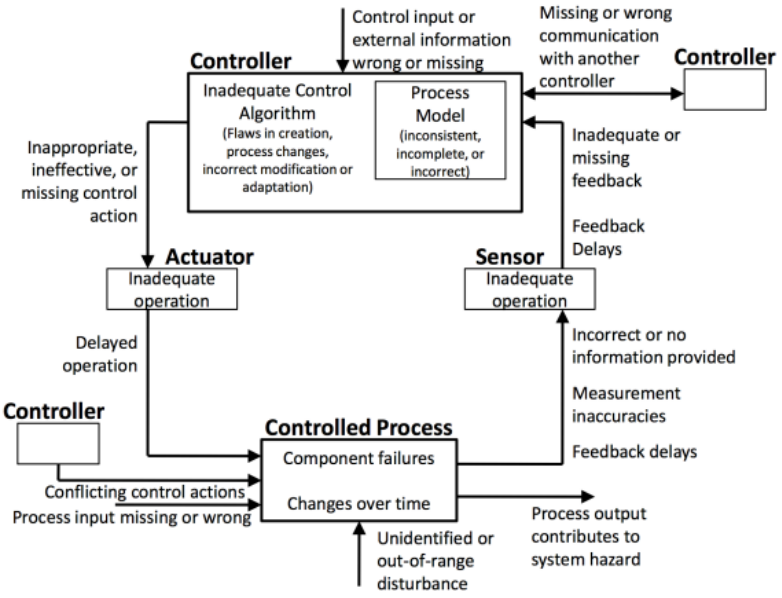
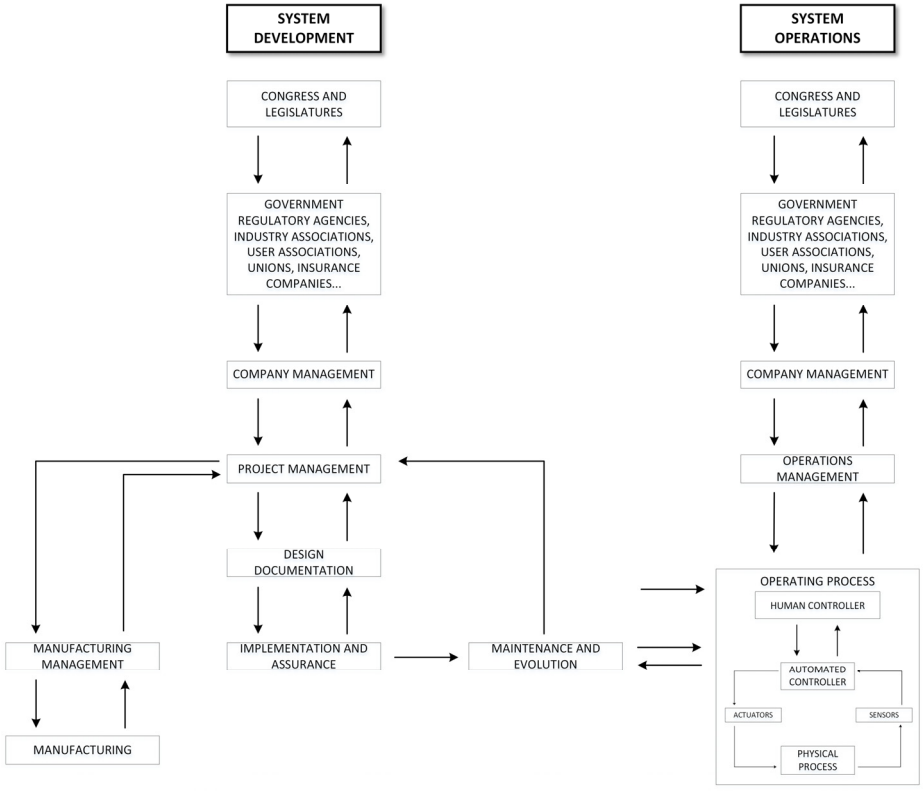


Figure 2 Example of socio-technical control structure (adapted from Leveson, 2011)



STPA is a hazard analysis method based on STAMP. STPA is a new hazard analysis technique with the same goals as any other hazard analysis technique, that is, to identify scenarios leading to hazards and thus to losses so they can be eliminated or controlled. However, STPA is based on systems theory while traditional hazard analysis techniques have reliability theory at their foundation.

The STPA applying procedure has four steps that are necessary to complete the process. The steps are (detailed in Leveson, 2011 and Leveson and Thomas, 2013) as follows:

1 Identify hazards and accidents.

2 Draw the control structure.

3 Identify potentially unsafe control actions.

4 Use the identified unsafe control actions to create safety requirements and constraints.

An unsafe control action (UCA) is the one that leads to a hazard. Leveson defines hazards as "A system state or set of conditions that together with a particular set of worst-case environmental conditions, will lead to an accident (loss)" (Leveson, 2011). In STPA there are four types of UCAs. On one hand, hazards can occur when a control action is 'provided' or 'not provided' and, on the other, when a control action has been carried out 'too late or too early' or it is provided 'too long or stopped too soon'. Thus, the first two types of UCAs are related to the control action status and the second two with the control action timing. Figure 1 allows for a systematic analysis of what factors can go wrong. The generic loop (applied identified control structure in step 2) is used mainly in step 3 and part in step 4.

2 Application of STPA to the chemical industry

2.1 A new approach

STAMP has been applied to different industries (nuclear, aviation, etc.), and it has been proposed as a promising methodology for the process industry (De Rademaeker et al., 2014) although there are no published works on how it should be applied in this industry. In this paper a new approach is suggested to apply STPA to the chemical and oil & gas industries. The application is focused on the lowest level of the control architecture, that is related to the equipment and process control loops. Upper control levels (human operators, alarms, maintenance, supervising, etc.) are not addressed and are the subject of a future paper. The main change to be done in the application of STPA to the process industry lies in step 3. The four unsafe control action types described in the previous section are enough for different domains but for chemical systems two extra unsafe control actions types are needed and have to be taken into account to enforce system safety.

Process plants are, usually, continuous plants and the control is achieved using conventional PID controllers that send the control action to the final element, typically a control valve. The operation of the valve is also continuous, and as it is not an On/Off controller (the valve is not just open/closed) the Provided/Not Provided UCAs are not

sufficient to describe the control action status. They have to be extended to include if the control action is more or less than it should be. So the UCAs for this system are 'provided' (we considered that provided means provided correctly, in the exact amount), More and Less (both of them constitute the Not Provided type). More or Less are directly related to the final value (after the control action) of the manipulated variable. In most of the cases the Less type effect includes the None effect on the process although there are some specific situations where None has to be specified besides the Less type. This could be considered as a third type of the Not Provided control action. For example if pressure is controlled in a vessel (hazard: high pressure) manipulating the exit stream a More control action is safe but a Less control action is unsafe as it means that gas is accumulating in the vessel. The reason to distinguish between more and less instead of leaving Not provided is because in some cases More can lead to a hazard and Less can lead to a different one in the same equipment.

Nowadays, STPA tables are individually generated for each UCA studying hazards for different scenarios (a scenario is a UCA along with context, not controlled, variables) (Leveson and Thomas, 2013). In the approach proposed herein, all UCAs are studied at the same time in the same table. Scenarios (context variables) are also discretised in 'Desired', 'None', 'Less' and 'More' (following the same UCA discretisation criteria). For real systems, the size of STPA tables will be huge (although less than using different tables for every UCA). The STPA Table Size (STS) can be calculated by equation (1):

$$STS = \prod_{i=1}^{\substack{\text{Number of}\\ \text{controlled}\\ \text{variables}}} \begin{pmatrix} \text{Number of UCAs} \\ \text{considered for } i \end{pmatrix} \prod_{j=1}^{\substack{\text{Number of}\\ \text{context}\\ \text{variables}}} \begin{pmatrix} \text{Number of states} \\ \text{considered for } j \end{pmatrix} \quad (1)$$

As it can be seen, the number of rows to evaluate in STPA tables can be huge. Therefore, some solutions are under development in order to automate the analysis process. One of them is the A-STPA open tool created by Asim Abdulkhaleq at the Institute of Software Technology, Stuttgart (Abdulkhaleq and Wagner, 2014).

Table 1 System engineering foundations of the process

Accident	*Hazard*	*Safety Constraint*
Explosion	H1: Temp too high	Temp must never violate maximum value

2.2 Example 1: a polymerisation reactor

The first process studied is a single reactor with only one control loop. The process is a batch polymerisation reaction. The reactor has two different feeds, one corresponds to the monomer (F_{mon}) and the other one corresponds to the initiator (F_{ini}) needed for the polymerisation reaction to occur. The reactor is cooled with an internal coil in which cooling water is circulated to control temperature (exothermic reaction). There is a single control loop to keep the reactor temperature manipulating the cooling water supply as shown in Figure 3 (Rodriguez and Diaz, 2014).

The size of the STPA table for this case is $4 \times 4 \times 4 = 64$ (one controlled variable, $TCV1$, and two context variables, F_{ini} and F_{mon}) rows (Table 2) that can be drastically reduced by removing all combinations intrinsically safe (Table 3). For example, in those cases where 'More' cooling water was supplied the system would be overcooled. It

would also happen when the cooling water would be supplied as required ('Provided'). If the refrigeration required is provided the system is always safe. Other examples of systems intrinsically safe are those where either the monomer or the initiator is not fed to the reactor. If one of the reactants needed is not present the reaction cannot be carried out, so temperature cannot rise. Besides, for this system, there are not differences between 'Less' and 'No' cooling water flow in terms of safety, so this cases would be studied together as 'Less'.

Figure 3 Process flow diagram of the polymerisation reactor

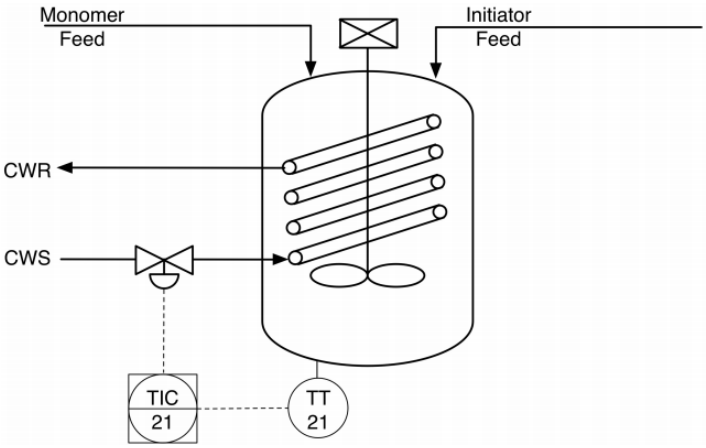


Table 2 STPA hazard analysis table of the polymerisation reactor

ID	F_{ini}	F_{mon}	*TCV1*	*Hazard?*
1	+	+	+	No
2	+	+	–	Yes
3	+	+	No	Yes
4	+	+	Provided	No
5	+	–	+	No
6	+	–	–	Yes
7	+	–	No	Yes
8	+	–	Provided	No
9	+	No	+	No
10	+	No	–	No
11	+	No	No	No
12	+	No	Provided	No
13	+	Desired	+	No
14	+	Desired	–	Yes
15	+	Desired	No	Yes

Table 2 STPA hazard analysis table of the polymerisation reactor (continued)

ID	F_{ini}	F_{mon}	*TCV1*	*Hazard?*
16	+	Desired	Provided	No
17	–	+	+	No
18	–	+	–	Yes
19	–	+	No	Yes
20	–	+	Provided	No
21	–	–	+	No
22	–	–	–	Yes
23	–	–	No	Yes
24	–	–	Provided	No
25	–	No	+	No
26	–	No	–	No
27	–	No	No	No
28	–	No	Provided	No
29	–	Desired	+	No
30	–	Desired	–	Yes
31	–	Desired	No	Yes
32	–	Desired	Provided	No
33	No	+	+	No
34	No	+	–	No
35	No	+	No	No
36	No	+	Provided	No
37	No	–	+	No
38	No	–	–	No
39	No	–	No	No
40	No	–	Provided	No
41	No	No	+	No
42	No	No	–	No
43	No	No	No	No
44	No	No	Provided	No
45	No	Desired	+	No
46	No	Desired	–	No
47	No	Desired	Not Provided	No
48	No	Desired	Provided	No
49	Desired	+	+	No
50	Desired	+	–	Yes
51	Desired	+	No	Yes
52	Desired	+	Provided	No

Table 2 STPA hazard analysis table of the polymerisation reactor (continued)

ID	F_{ini}	F_{mon}	*TCV1*	*Hazard?*
53	Desired	–	+	No
54	Desired	–	–	Yes
55	Desired	–	No	Yes
56	Desired	–	Provided	No
57	Desired	No	+	No
58	Desired	No	–	No
59	Desired	No	No	No
60	Desired	No	Provided	No
61	Desired	Desired	+	No
62	Desired	Desired	–	Yes
63	Desired	Desired	No	Yes
64	Desired	Desired	Provided	No

Table 3 Reduced STPA hazard analysis table

ID	F_{ini}	F_{mon}	*TCV1*	*Hazard?*
1	+	+	–	Yes
2	+	–	–	Yes
3	+	Desired	–	Yes
4	–	+	–	Yes
5	–	–	–	Yes
6	–	No	–	No
7	–	Desired	–	Yes
8	Desired	+	–	Yes
9	Desired	–	–	Yes
10	Desired	Desired	–	Yes
11	No	All	All	No
12	All	No	All	No
12	All	All	+	No
12	All	All	Provided	No

To illustrate the differences with respect to HAZOP studies, only the cooling water supply (CWS) line is commented here. From HAZOP, if NO guide word is applied to variable FLOW in CWS line, HAZOP results in a hazard of a possible temperature rise. The next step in HAZOP analysis would result in some recommendations to be implemented in the safety instrumented system (SIS). That, in principle, should agree with some of STPA proposed solutions. From STPA analysis, as shown in Tables 2 and 3, not all the cases are necessarily hazardous. For example, there are different scenarios in which 'Less/No' flow are safe scenarios. So, in other words, STPA analysis results not only in the detection of hazardous situations but also in the potential solutions that can be implemented in SIS. So the solution (to force a safe scenario) when cooling water valve is not open would be to close reactive flows.

Figure 4 Process flow diagram of the process

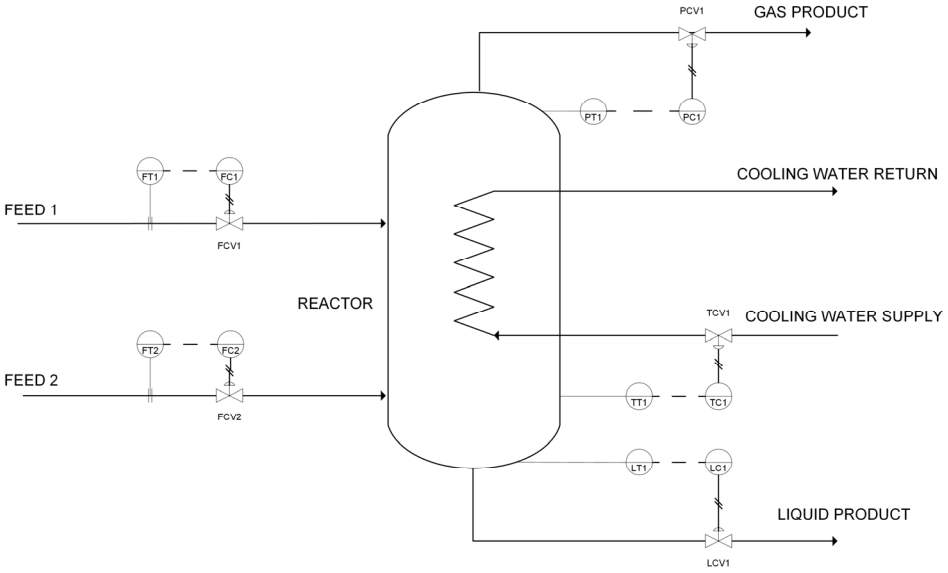


Table 4 System engineering foundations of the process

Accident	*Hazard*	*Safety Constraint*
Explosion	H1: Temp. too high	Temp. must never violate maximum value
	H2: Pressure too high	Pressure must never violate maximum value
Leakage	H3: Level too high	Level must never violate maximum value

2.3 Example 2: a generic exothermic reactor

The system studied is an exothermic reactor where a vapour stream (Feed 1) and a liquid stream (Feed 2) are fed to the reactor. The products of the reaction are also in vapour and liquid phase so two outlet streams are present. The system is pressurised (about 30 bar) to improve gas solubility into the liquid. This can be achieved by controlling pressure, manipulating the flow rate of the top gas product stream. On the other hand, liquid level in the reactor is also controlled by means of bottom liquid product flow rate. The reaction is carried out at constant temperature (around 200°C) so an internal heat exchanger (coil) is required. Temperature is kept by changing cooling water flow rate.

First of all it can be remarked the big size of STPA (Table 5) as the complexity of the system increases. In this case, for five controllers, it is necessary to carry out 243 individual analyses. And it is just for one unit, so one of the main limitations expected for STPA analysis is the great number of rows for the tables, although the table can be reduced following the same approach described earlier. Therefore, great efforts are being done to automatise table generation and analysis. Our approach under development is through functional modelling (Rodriguez and Diaz, 2014).

Table 5 STPA hazard analysis table of the polymerisation reactor

ID	*FCV1*	*FCV2*	*PCV1*	*TCV1*	*LCV1*	*Hazard*
1	+	+	+	+	+	No
2	+	+	+	+	–	H3
4	+	+	+	+	Provided	No
...	...	...	...	...	...	...
85	+	–	+	–	+	No, only if '–' in *FCV2* means no flow. If less flow H1
...	...	...	...	...	...	...
103	–	–	+	–	+	No only if '–' in either *FCV2* or *FCV1* means no flow
...	...	...	...	...	...	...
181	–	–	+	+	+	No
182	–	–	+	+	–	H3
183	–	–	+	+	–	No
184	–	–	+	+	Provided	No
185	–	–	+	–	+	No, only if '–' in either *FCV2* or *FCV1* means no flow. If less flow H1
...	...	...	...	...	...	...

When all STPA analysis is available, much extra information is obtained compared to HAZOP. As an example, again for the cooling system it can be seen that the system is not always unsafe when no cooling water is supplied (ID 85), and also we have identified a great set of safe scenarios. That means that we can also 'measure' how far our situation is from any of all safe scenarios and take minimum actions in order to force the system to the *closest safe scenario*.

2.4 HAZOP comparison

In order to provide a comparison with traditional HAZOP studies, let's consider the following example of a HAZOP application: the oil vaporiser. This is documented in international standards (BSI Standards, 2001) and shown in Figure 5. In this example, the hazards taken into account are H1: high temperature and H2: high pressure in the vaporiser (Table 6).

If three UCAs (Provided, LESS, MORE) are applied to each control action, it would result in $3^4 = 81$ rows in STPA table. However, some cases are not applicable and can be avoided in order to reduce STPA table size. For example, for the interlock actions only 'Provided' and 'Not Provided' (LESS) will be taken into account according to interlock logic implementation. The number of cases to be studied is $3 \times 3 \times 3 \times 2 = 54$. Besides, all cases in which interlock control action is not provided are themselves unsafe. For all those cases, H1 is present. Therefore, they are eliminated from the STPA so the number of cases to be studied is $3 \times 3 \times 3 = 27$.

Figure 5 Process flow diagram of the oil vaporiser

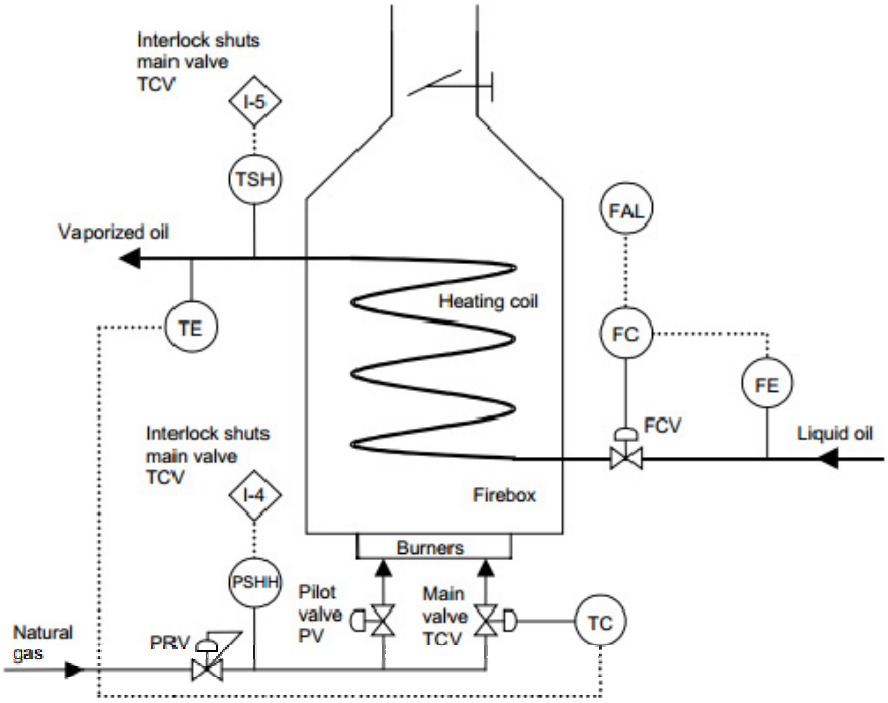


Table 6 System engineering foundations of the process

Accident	*Hazard*	*Safety Constraint*
Explosion	H1: Temp. too high	Temp. must never violate maximum value
	H2: Pressure too high	Pressure must never violate maximum value

From HAZOP (BSI Standards, 2001) the installation of a low flow alarm in the liquid oil stream as one of the main suggested recommendations. As it can be seen in Table 7, it can also be deduced from STPA analysis (rows 19 to 27) that a lower liquid flow rate is related with H1 (increased temperature). Once again, the closest safety state is given. For example, it is proposed that one solution for situation 19 would be 21 with no flow through PRV. This means closing the PRV or, easier, closing the valve associated to TC1 (ID 25).

Nevertheless, although for the situations studied, STPA is a superset of HAZOP resulting in a deeper study of the system with extra information given, HAZOP provides other information related to other key words applied but not taken into account in this work. For example, when applying *'Other than'* to the liquid oil stream, an evaluation of the influence on vaporiser behaviour of other types of material different from oil (i.e. water) is studied. A way to introduce this kind of situation in a STPA study could be by defining a new hazard associated with the new situation ('water is present'), add the control structure associated (if exists) and then analyse new UCAs together with the existing ones.

Table 7 STPA hazard analysis table of the oil vaporiser

ID	*FC1*	*TC1*	*PRV*	*Hazard*
1	Provided	Provided	Provided	No
2	Provided	Provided	+	H2
3	Provided	Provided	–	No
4	Provided	+	Provided	H1
5	Provided	+	+	H1, H2
6	Provided	+	–	H1. No hazard if '–' in *PRV* means no flow
7	Provided	–	Provided	No
8	Provided	–	+	No
9	Provided	–	–	No
10	+	Provided	Provided	No
11	+	Provided	+	No
12	+	Provided	–	No
13	+	+	Provided	H1
14	+	+	+	H1, H2
15	+	+	–	No
16	+	–	Provided	No
17	+	–	+	No
18	+	–	–	No
19	–	Provided	Provided	No
20	–	Provided	+	H2
21	–	Provided	–	H1. No hazard if '–' in *PRV* means no flow
22	–	+	Provided	H1
23	–	+	+	H1, H2
24	–	+	–	H1. No hazard if '–' in *PRV* means no flow
25	–	–	Provided	H1. No hazard if '–' in *TC1* means no flow
26	–	–	+	H1, H2. No hazard if '–' in *TC1* means no flow
27	–	–	–	H1. No hazard if '–' in either *PRV* or *TC1* means no flow

3 Conclusions

This paper has applied the STPA methodology to the lowest level of chemical process control architecture. Through several examples it has been shown that STPA can potentially replace, or at least complement, HAZOP as the hazard analysis technique for chemical and oil& gas industries. Although the differences between the two techniques are not so important in the lowest level, the great advantage of STPA lies in its systemic nature (i.e. it can assess hazards involving interactions between system parts). Another advantage of STPA is that, in the examples studied, it can be seen that it can give the solution too (closest safe scenario). Besides it is better to apply STPA than HAZOP because the low level analysis could be coupled with the high level analysis (human and organisational factors). This will be the topic of a future paper of our group.

A problem found when the approach proposed is applied, is the great size of the resulting tables. It is needed to develop a tool in order to simplify the analysis. It can be done by applying functional modelling as a way to automate the analysis of some (or all) cases. Since 2009 (Rodriguez and Sanz, 2009), we are working on the development and application of the functional modelling technique called D-higraphs. Specifically, we are working now on the way D-higraphs can improve the applicability of STPA to chemical processes.

References

Abdulkhaleq, A. and Wagner, S. (2014) 'A-stpa: open tool support for system-theoretic process analysis', in MIT (Ed.): *STAMP Workshop 2014*.

BSI Standards (2001) *Hazard and operability studies (HAZOP studies). Application guide*, Technical report, British Standard.

Center for Chemical Process Safety (1999) *Guideline for Hazard Evaluation Procedures*, Technical report, AIChE, New York, NY.

De Rademaeker, E., Suter, G., Pasman, H.J. and Fabiano, B. (2014)' A review of the past, present and future of the European loss prevention and safety promotion in the process industries', *Process Safety and Environmental Protection*, March.

Dunjó, J., Fthenakis, V., Vlchez, J. and Arnaldos, J. (2010) 'Hazard and operability (HAZOP) analysis. A literature review', *Journal of Hazardous Materials*, Vol. 173, Nos. 1–3, pp.19–32.

Hollnagel, E., Woods, D.D. and Leveson, N. (2006) *Resilience Engineering: Concepts And Precepts*, Ashgate.

Leveson, N.G. (2011) *Engineering a Safer World. Systems Thinking Applied to Safety*, The MIT Press.

Leveson, N.G. and Stephanopoulos, G. (2014) 'A system-theoretic, control-inspired view and approach to process safety', *AIChE Journal*, Vol. 60, No. 1, pp.2–14.

Leveson, N.G. and Thomas, J. (2013) *An STPA primer*, Technical report, Massachusetts Institute of Technology, Boston.

Mannan, S. (2004) *Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, Elsevier Science & Technology Books.

Nimmo, I. (1995) 'Abnormal situation management', *Process and Control Engineering*, Vol. 49, No. 5.

Pasman, H.J. (1998) '50 years of improvement to safety', in NRIFD (Ed.): *Proceedings of International Workshop on Safety in the Transport, Storage and Use of Hazardous Materials*, Tokyo, Japan.

Rasmussen, J. and Svedung, I. (2000) *Proactive Risk Management in a Dynamic Society Proactive Risk Management*, Swedish Rescue Services Agency, Karlstad, Sweden.

Rodriguez, M. and Diaz, I. (2014) 'A new functional systems theory based methodology for process hazards analysis', *Computer-Aided Chemical Engineering*, Vol. 33, pp.703–708.

Rodriguez, M. and Sanz, R. (2009) 'Modeling using higraphs: an integrating approach', *Computer-Aided Chemical Engineering*, Vol. 26, pp.871–876.

Venkatasubramanian, V. (2011) 'Systemic failures: challenges and opportunities in risk management in complex systems', *AIChE Journal*, Vol. 57, No. 1, pp.2–9.