Journal of Loss Prevention in the Process Industries xxx (2016) 1–9

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

A systematic and integral hazards analysis technique applied to the process industry

Manuel Rodríguez*, Ismael Díaz

Dpto. Ingeniería Química Industrial y del Medio Ambiente, ETS Ingenieros Industriales, Universidad Politécnica de Madrid, C/José Gutiérrez Abascal 2, Madrid, 28006, Spain

ARTICLE INFO

Article history:
Received 26 February 2016
Received in revised form
21 June 2016
Accepted 23 June 2016
Available online xxx

Keywords:
Hazard analysis
Systems theory
Process industry
STAMP
STPA

ABSTRACT

Traditional approaches to process safety are not enough. Accidents keep occurring every day across the globe. Technology advances make systems more complex and their behaviour more non linear and unpredictable. This trend will increase in the coming years mainly due to the new industrial paradigm that will change production processes to fully digital. In this context this paper analyses the current status and methodologies and introduces the need to change to systems theory based approach for process safety. An overview of different system theory based techniques is presented. A more in deep explanation is given about the STAMP-STPA methodology. Finally, STPA is applied to a case study of the process industry pointing out the needs, advantages and drawbacks of the approach.

1. Introduction

1.1. Safety a present and actual problem

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 have showed 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 thirty years usually driven by important accidents (Flixborough, 1974; Seveso, 1976; Three Mile Island, 1979; Bhopal, 1984). These have caused widespread public concerns about major incidents in chemical plants, Mannan (2004). Besides the regulations, accidents keep occurring. As a curious fact, the first big accident happened in 1921 September the 21st in an ammonium nitrate plant in Oppau (Germany) and the very same day 80 years after a big accident happened again in an ammonium nitrate plant in Toulouse (France). Today you can find many accidents happening in the process industry everyday which are reported in the Abnormal Situation Management Consortium web page.

The main problems present currently in the process industry regarding safety, according to Mannan et al., (2010), are basically:

- Organizations have no memory of past accidents.
- Insufficient attention to leading indicators.
- Process operations with increasing complexity.
- Need for better solutions and approaches.

The last item is nowadays widely accepted as indicated in De Rademaekeret al. (2014).

1.2. Causes of accidents

Technology is rapidly evolving and the process industry, although at a lower pace, is being affected by it. Today, process plants involve operations with complex human-machine interactions. The processes are large, complex, distributed, and more automated. There are a lot of interactions and couplings between sub-systems and equipment, and computers (software) play a

* Corresponding author.
E-mail address: manuel.rodriguezh@upm.es (M. Rodríguez).

http://dx.doi.org/10.1016/j.jlp.2016.06.016
0950-4230/

significant role in the human-machine interaction Soken et al. (1995). The social part of the systems has a very important role which means that now not only the technical but the complete socio-technical structure has to be taken into account. Team members (managers, supervisors, operators, etc.) have to cope with heterogeneous and sometimes conflicting information, performance pressure and high workload, Bullemer and Laberge (2010). Table 1 shows top 3 common failures found by Bullemer after analysing more than 30 incidents.

2. The traditional approach to safety

2.1. The traditional approach

One of the first methodologies for safety was Failure Mode and Effects Analysis (FMEA) that dates from the end of the 40's but most traditional techniques appeared in the 60's: Fault Tree Analysis (FTA), Hazard and Operability study (HAZOP), Event Tree Analysis (ETA) and Bow Tie – early 70's. All these tools used to identify hazards (defining hazard as a set of *chemical*, *physical or changing conditions that have the potential for causing damage* Center for Chemical Process Safety (1999)) share a common view and it is that they consider accidents caused by component failures, following a chain of events.

In the process industry the de facto standard is HAZOP, developed by ICI. 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).

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.
- Time consuming and expensive.
- Both human and organizational factors are rarely taken into consideration and only related to lower levels in the organizational hierarchy.

As stated earlier, safety is considered a failure problem so the way to protect a system, after conducting the hazards analysis, is to add a set of barriers. In order to do this after the HAZOP study a method to calculate the safety integrity level (SIL) is conducted. A widely used methodology for this is the Layers of Protection Analysis (LOPA). With this protection in place, for an accident to happen a chain of failures passing through the barriers is needed The protection layers can be classified into prevention and mitigation layers. Fig. 1 shows the onion-like system used in the process industry.

With this protection in place for an accident to occur there has to be "aligned holes" in all the layers so it seems that with all these protective layers an accident should almost never happen (based on reliability the accident has a very low probability), but unfortunately this is not the case. It appears then that the prevailing assumption of classical models that accidents are caused by a chain of directly related events is not the proper way to tackle the problem. At least it is not enough and new complementary techniques are needed. As stated in Leveson (2011a,b) safety is not the same as reliability, one does not imply nor require the other—a system can be reliable and unsafe or safe and unreliable. In some cases, these two system properties are conflicting.

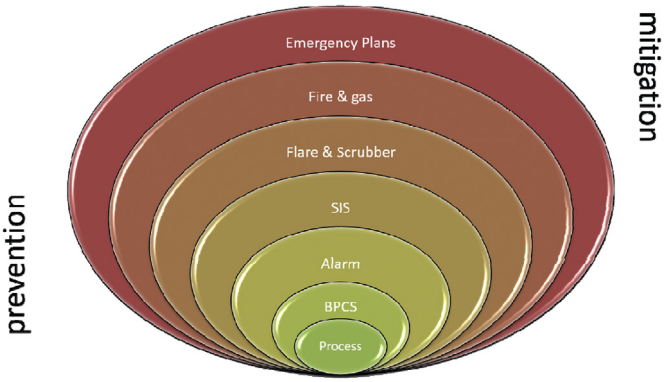

Fig. 1. Layers of protection in the process industry.

2.2. Why the traditional approach is not enough

We have claimed in the previous section that reliability is not enough to guarantee safety, almost 20 years ago Pasman (1998) extracted some conclusions from the analysis of past accidents:

- 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.

Following these conclusions we present additional reasons that support our previous claim:

1. Systems are becoming more complex (being software the main contributor) which means:
   a. There are accidents that result from interactions among components not just from component failures (Venkatasubramanian (2011)).
   b. The increasing complexity impedes to anticipate all potential interactions.
   c. Component interactions are usually non-linear and their behaviour is difficult to predict.
2. Traditional techniques omit or oversimplify some important factors:
   a. Human factor. This is a crucial element when considering safety, although some methodologies, like HAZOP, can consider human errors when applied, they only do it to a

Table 1
Top 3 common failures across all the incidents (Bullemer and Laberge (2010)).

Common failure modes	Freq.	%
Implement a comprehensive hazard analysis and communication program	79	15
Establish effective first line leadership roles to direct personnel, enforce organizational policies and achieve business objectives	65	12
Establish an effective and comprehensive program to continuously improve the impact of people, equipment, and materials on plant productivity and reliability	60	11

Please cite this article in press as: Rodríguez, M., Díaz, I., A systematic and integral hazards analysis technique applied to the process industry, Journal of Loss Prevention in the Process Industries (2016), http://dx.doi.org/10.1016/j.jlp.2016.06.016