Safety Science 101 (2018) 209–219

Contents lists available at ScienceDirect

Safety Science

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

Employing process simulation for hazardous process deviation identification and analysis

Rafael Raoni[a,b,*], Argimiro R. Secchi[a], Micaela Demichela[b]

[a] Chemical Engineering Program-COPPE, Universidade Federal do Rio de Janeiro, Cidade Universitária, Centro de Tecnologia, 21941-914 Rio de Janeiro, RJ, Brazil
[b] Department of Applied Science and Technology, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy

A R T I C L E I N F O

Keywords:
Hazard analysis
Process simulation
Process deviation
Systematic procedure
Heuristic analysis

A B S T R A C T

To improve industrial safety, several hazard analyses of processes are available. The HAZOP is one of the most frequently employed and analyzes hazardous process deviations based on heuristic knowledge. Despite the wide application of the technique, new developments are especially important to enhance industrial safety. In this sense a systematic procedure is proposed for hazardous process deviation identification and analysis that employs process simulation and heuristic evaluation. Process simulation enables the analysis of process behaviors caused by device malfunctions and the performance of deviation analysis that considers the process non-linearities and dynamics. A comparison between the HAZOP and the proposed procedure is presented using a pump startup system case study, wherein the better system interpretation and results regarding abnormal process conditions are highlighted. A second case study applies the procedures to an offshore oil production process, showing the advantages of employing process simulation for studying deviation during a dynamic process's abnormal behavior.

1. Introduction

Several techniques are available to identify and analyze hazardous conditions. A rigorous and systematic procedure followed by a multidisciplinary team of experts is widely employed in different methods of hazard identification (Crowl and Louvar, 2002; Mannan, 2005). In the framework of process hazards, the HAZOP (*hazard operability*) study (Kletz, 1997; Lawley, 1974; Swann and Preston, 1995; Tyler, 2012) is one of the most recognized and widely used studies in industries (Tyler, 2012), and techniques such as FMEA (*failure mode and effect analysis*) (Kenneth, 2004; McDermott et al., 2009) are also widely used for the identification of hazards caused by failure modes of equipment and processes. Furthermore, in terms of probabilistic risk assessment, several other techniques are available, of which the fault tree (FT) is one of the most often employed (Chiacchio et al., 2011; Siu, 1994).

Given the importance of identifying and analyzing industry hazards, it seems reasonable to improve the quality of hazard assessment by mixing the concepts of different risk analyses, such as the ROA (Demichela et al., 2002), which integrates the concepts of the HAZOP for hazard identification and the FT for frequency assessment. Furthermore, considering the HAZOP as one of the most important hazard analyses in process industries, some of its insights and improvements are introduced.

1.1. Description of traditional HAZOP

Basically speaking, the method examines the plant documentation with the aim of identifying the hazardous consequences of recognized process deviations (Dunjó et al., 2010) as well as being a source of information for further quantitative risk analysis (Demichela et al., 2002; Siu, 1994). The technique's power lies in its procedure for generating process deviations (e.g. high pressure), which combines guide words (high, less, none, etc.) and process variables (pressure, temperature, etc.). The analysis is carried out considering deviations at the identified nodes, referred to as plant sections, in which the process variables' behavior is analyzed to allow the identification of the causes, consequences and safeguards of the deviation. Furthermore, following some reference tables, the qualification of the scenario risk may be made for a certain risk focus (e.g. the environment, people, image and assets) and, when necessary, some observations or recommendations may be offered (Dunjó et al., 2010) to improve the process's safety concerning the identified hazard.

The systematic procedure enables the identification of all the possible deviations of the system (Crowl and Louvar, 2002), which,

* Corresponding author at: Chemical Engineering Program-COPPE, Universidade Federal do Rio de Janeiro, Cidade Universitária, Centro de Tecnologia, 21941-914 Rio de Janeiro, RJ, Brazil.
E-mail addresses: rbritto@peq.coppe.ufrj.br (R. Raoni), arge@peq.coppe.ufrj.br (A.R. Secchi), micaela.demichela@polito.it (M. Demichela).

http://dx.doi.org/10.1016/j.ssci.2017.09.014
Received 9 April 2017; Received in revised form 13 July 2017; Accepted 19 September 2017
0925-7535/

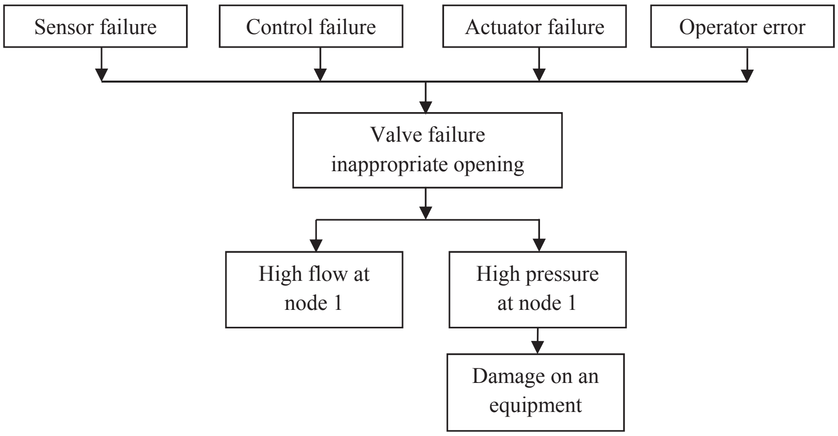

Fig. 1. Sequence of undesired events caused by a valve failure.

depending on its dimension, may be divided into smaller subsystems to facilitate a manageable analysis. The method is employed during long-time meetings with a multidisciplinary group of specialists and requires a large amount of time and work (Khan and Abbasi, 1997; Swann and Preston, 1995). Its quality strongly depends on the capability of the safety specialist who guides the study, on the expertise of the multidisciplinary group and on the group's capability to maintain accuracy until the end of the study.

1.2. Computational advances in hazard analysis

Despite the wide application of heuristic hazard analyses, some efforts have been made to make computational advances in hazard assessment techniques. Aiming to improve the HAZOP team efficiency, so-called expert systems have been studied widely (Dunjó et al., 2010) and implemented in many commercial tools. The main idea of the proposals is to analyze the propagation of the deviation throughout an empirical model of the system (Bartolozzi et al., 2000; Boonthum et al., 2014; Cocchiara et al., 2001; Cui et al., 2010; Leone, 1996; Wang and Gao, 2012), generating an "automatic HAZOP" requiring less time (Boonthum et al., 2014) and providing constant quality during the whole analysis and improved consequence identification due to the deviation propagation throughout the system model (Bartolozzi et al., 2000). Accordingly, the deviation propagation may use, among others, a petri network (Chung and Chang, 2011; Srinivasan and Venkatasubramanian, 1998a, 1998b) or fuzzy logic (Guimarães and Lapa, 2005).

Other works have considered computational process dynamic simulation for hazard study to investigate the emergency process conditions (Shacham et al., 2004), for operators training in emergency situations (Eizenberg et al., 2006b) and to identify the conditions in which safeguard activation occurs (Demichela and Camuncoli, 2013). The use of dynamic simulation for deviation analysis has been employed in an extended HAZOP approach (Ramzan et al., 2006), making possible the identification of non-trivial consequences and better system safeguards (Li et al., 2010). Furthermore, the importance of simulation has been highlighted for hazard analysis of non-linear processes with multiple steady states (Labovsky et al., 2007; Svandova et al., 2005), in which an improved quantitative and sensitive deviation analysis is required. In these latter works, it was exemplified that a small deviation can cause substantial process disturbance, highlighting the advantages of quantitative versus qualitative deviation analysis.

Both expert system and process simulation aim to overcome some of the difficulties faced during a heuristic hazard analysis. Given the complexity of process plants, it seems logical to use process simulations to understand hazardous process conditions and to implement computational advances to automate a known systematic approach. On the other hand, since not all anomalous process behaviors can be predicted or implemented in computational software, the importance of expert opinion for hazard analysis is highlighted. In this sense a procedure that groups both computational advances and expert opinion seems important to improve the process safety.

In this work a systematic procedure that uses process simulation is proposed for the identification and analysis of hazardous process deviation. The procedure presents steps that can be automatized computationally and is concluded in multidisciplinary meetings. The hazard scenario is defined as one possible malfunction of devices (process units), which must be simulated to identify the group of its dependent process deviations. Such information is grouped and feeds a further heuristic process hazard analysis that aims to overcome the limitations of the computational tools. In Section 2 the proposed procedure is described; in Section 3 two case studies that aim to exemplify the procedure's application, results and technical improvements are provided; and in Section 4 the conclusion of the work is presented.

2. Proposed procedure

2.1. Procedure description and process boundaries

During normal operation, with proper action of the process devices, no problems arise. Then an abnormal system condition occurs when a particular device does not operate as originally expected. To give an example, the inappropriate opening of a control valve is an abnormal system condition that could be caused by previous events and leads to several further undesirable consequences, including some process deviations. Such an example, shown in Fig. 1, represents a sequence of process behaviors in terms of cause–consequence assumptions, which could be extended by previous causes and further consequences until the desired level of detail is reached. Therefore, to propose a manageable procedure, it is necessary to determine the boundaries of the process to be analyzed.

Aiming to identify process deviations, the identification of their causes is defined as the starting point of the proposed analysis, and, the inappropriate manipulation of devices being the major cause of process deviations, a study of the devices' malfunction is needed. In this sense, despite the possibility of using any kind of procedure, the FMEA could be understood as a good choice to identify devices' inappropriate manipulation. Moreover, during this identification attention must be paid to identifying device malfunctions that change the normal process condition, which must include the identification of common cause failures. Furthermore, the analysis of these changes during the normal process condition enables the identification of process deviations and further consequences. In addition, after an inappropriate device malfunction, the transient behavior of the process determines the necessary time until the occurrence of the process deviations and their further consequences, leaving room for interventions from the system