Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better?

Ian Cameron[a], *Sam Mannan*[b], *Erzsébet Németh*[a], *Sunhwa Park*[b], *Hans Pasman*[b,*], *William Rogers*[b], *Benjamin Seligmann*[c]

[a] *School of Chemical Engineering, The University of Queensland, Brisbane, Queensland, Australia*
[b] *Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chem. Eng., Texas A&M University, College Station, TX, USA*
[c] *Department of Chemical Engineering, Curtin University, Perth, Western Australia, Australia*

ARTICLE INFO

Article history:
Received 25 November 2016
Received in revised form 21 January 2017
Accepted 25 January 2017
Available online 3 February 2017

Keywords:
Process hazards
Hazard identification
HAZOP automation
Scenario generation
System approach
Dynamic Bayesian net

ABSTRACT

Hazard identification is the first and most crucial step in any risk assessment. Since the late 1960s it has been done in a systematic manner using hazard and operability studies (HAZOP) and failure mode and effect analysis (FMEA). In the area of process safety these methods have been successful in that they have gained global recognition. There still remain numerous and significant challenges when using these methodologies. These relate to the quality of human imagination in eliciting failure events and subsequent causal pathways, the breadth and depth of outcomes, application across operational modes, the repetitive nature of the methods and the substantial effort expended in performing this important step within risk management practice. The present article summarizes the attempts and actual successes that have been made over the last 30 years to deal with many of these challenges. It analyzes what should be done in the case of a full systems approach and describes promising developments in that direction. It shows two examples of how applying experience and historical data with Bayesian network, HAZOP and FMEA can help in addressing issues in operational risk management.

1. Introduction

All safety considerations start with recognizing possible hazard events, hence the necessity of hazard identification (HI) via process hazard analysis (PHA). Hazard identification has the objective of defining all possible (*non possumus*) scenarios or sequences of events in which a hazard with its associated chance of realization will generate risks to people, assets, environment or corporate reputation. The potential causing the hazardous situation can reside within the system for a long time or could result from a set of temporal conditions.

PHA is a basic step towards risk assessment and risk management of a technical system and its process. Throughout the history of process design and operation much was learned by trial and error. Today, properties of materials are not regarded as a problem but 50 years ago they were. Many test methods did not yet exist. Phenomena such as runaway or vapor cloud explosion were unknown. Although sound knowledge of the material properties is a first requirement for a PHA, a *conditio sine qua non*, we shall assume for this paper that it is adequately represented, and we shall focus on finding out "*how things can go wrong*".

Early-on, it became already clear that an individual person is not able to think of all possible ways a mishap can occur. The first more or less formal method to evaluate plant process safety was application of a *checklist* based on experience. It required investigating properties of substances, reaction patterns, equipment hazards, safety devices, storage and loading, plant layout, emergency planning and the like. Another, even less formal and perhaps older method is '*What-if?*' For example: what-if valve V1 is shut, while it should be open?

Subsequently, a systematic, scenario oriented method appeared, which was designated Hazard and Operability Study (HAZOP). Accord-

* Corresponding author.
E-mail address: hjpasman@gmail.com (H. Pasman).
http://dx.doi.org/10.1016/j.psep.2017.01.025

ing to a paper in the 1971 Newcastle Major Loss Prevention in the Process Industries Symposium by Houston (1971) of Imperial Chemical Industries (ICI.), UK, in the case of a new design, safety was initially judged by "how well it will work". As existing codes of practice fell short, for a new design an "Operability Study" was undertaken. Based on a flow sheet, and later a Piping & Instrumentation Diagram (P&ID), a team of experts systematically examined line by line for possible process deviations, and if one was found, what would cause it, and what would be the consequence. Process deviations from design intent were investigated following a brief checklist of guide words, such as More, Less, etc., with the main ones as we know them from today's HAZOP (Hazards and Operability).

In his 1997 article on HAZOP, Trevor Kletz (1997), also in ICI at the time, mentioned more details. The HAZOP inception was in 1963/1964 on a new phenol plant design minimized with respect to capital cost, and the team that should operate the plant was given the assignment to perform a 'Critical Examination'. The latter was known at the time as a formal method asking questions, what is achieved, what else could be achieved, what should be achieved, how, when, and who has achieved it. A team of three worked three days a week for four months and found many operating problems and hazards. It later turned out that elsewhere in ICI the same critical examination technique had been applied before. From this, HAZOP as a formal method emerged and conquered the chemical process world and beyond to across a large variety of design activity. However, even in the first journal publication Lawley (1974), also at ICI, it was separately called the Operability study method and the Hazard analysis method. The method became formalized and an extensive literature evolved on how to efficiently apply it. Dunjó et al. (2010) has summarized the history, the literature of how best to perform HAZOP, as well as the attempts to include human failure and other aspects and applications.

Another systematic method that found general application is Failure Mode and Effect Analysis (FMEA) to which Criticality Analysis (FMECA) can be added to increase its rigor. The method started in 1949 as a military procedure in MIL-P-1629 "Procedures for Performing a Failure Mode, Effects and Criticality Analysis". Navy-Air converted it to standard MIL-STD-1629 in 1974, being further developed to version A in 1980. The method was applied in design in aerospace and then spread to other industries. Basically, from a piece of equipment the failure modes and their effects shall be identified, subsequently the causes and controls to prevent, and actions to be executed. FMECA, although applied basically as a reliability engineering tool according to the standard, found application too in maintainability, safety analysis, survivability and vulnerability, logistics support analysis, maintenance plan analysis, failure detection, and isolation sub-system design. Hence, where HAZOP is oriented towards operational function as seen in the systems states of temperature, pressure, flow and the like, FMEA is centered on component function and failure. These two methods overlap.

There are many more identification methods created for specific system purposes. These include approaches such as Taylor's action error analysis (Taylor, 2013), which is a kind of HAZOP on potential operator errors, or sneak analysis developed for electronic circuitry fault finding. A huge range of human factors methods have been developed over the last 25 years (Stanton et al., 2005). However, these methods have generally never reached the level of application in the process industries as have HAZOP and FMEA.

Meanwhile, in many countries, major hazard facilities and other process installations are required by law to not only perform hazard identification before the start of operations but also on a regular, repeating basis such as 5 years for the life of the installation. This requirement signifies the importance of the activity. Missing a scenario and therefore not being prepared to prevent and counter the undesirable outcomes may lead to disaster.

In summary, process hazard analysis (PHA), hazard identification (HI) and scenario definition form the cornerstone of the safety management system, and this is a team effort based on knowledge, experience, and human imagination of what can go wrong. In the next section we review the limitations of current methods due to the considerable effort, expense and the potential weaknesses in human imagination. Following that, we formulate some research questions and ways to improve hazard identification and to enhance the effectiveness and efficiency of the effort.

This paper was inspired by two CET published conference papers for the 15th International Symposium on Loss Prevention and Safety Promotion in the Process Industries 2016 in Freiburg, Germany, respectively, the one of Pasman and Rogers (2017) and that of Cameron et al. (2016).

2. Current challenges and limitations

In considering the question:

> "Are the conventional tools sufficient, or should and can we do much better?",

it is helpful to discuss what is meant by "sufficient", and what constitutes "much better".

First, in relation to '*sufficiency*' or meeting stated needs, practical application of techniques, such as HAZOP or FMEA, over many decades have certainly given excellent insights into the integrity of process designs and important operational aspects. However, these techniques have often been judged as not meeting needs for a variety of reasons, which are inherent in the methodologies and the particular manner in which they are applied. This is particularly evident in major accident reviews where deficiencies in HI were regarded as a major contributing factor in the accident.

The shortcomings can include: a lack of breadth and depth of analysis, a lack of team diversity and imagination, tedium, exhaustion, effort and expense, effective capture and communication of outcomes, follow through to final consequences, poor prioritization of associated risks, handling multiple operating modes, interaction with people and procedures, and the effectiveness of outcomes on decision making as HI outcomes are passed across various organizational groups (Kletz, 2009). All these issues can diminish the '*sufficiency*' of the method and its applications: in some cases, with disastrous outcomes.

Second, there appears little objection against the idea that we should be doing better than the current situation. Past development efforts have focused on some of these issues with varying degrees of success. Others have stalled due to internal policies and procedures of companies that do not wish to disrupt existing practices and who remain to be convinced of the benefits of change.

Third, it is evident that with a growing focus on life cycle perspectives, accompanied by significant advancement in information and communications technologies (ICT), there are many opportunities to "*do much better*". Exploiting systems thinking and ICT advancements can drive beneficial change. What follows discusses these issues.

Since HAZOP is the main tool to identify scenarios, we focus on its limitations. In the first place there is the limitation in effort capacity. Conducting a HAZOP is labor intensive. To not lose focus, a team of five should work only half days on a project. Each P&ID requires about 5×20 h, and for a plant depending on size 1–6 weeks may be required for a HAZOP. As this must be performed in the design stage, once more before commissioning, and every five years after being in operation, the effort and costs add up. Meanwhile the results usually sit on a shelf and are not used in day-to-day operations; this also reduces its cost effectiveness.

Serious, however, are the limitations due to the range of personnel abilities and the quality of effort that can lead to the missing of key hazard scenarios. Baybutt (2015a) in one of his