Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Automated HAZOP revisited

J.R. Taylor

Department of Management Engineering of the Technical University of Denmark, Denmark

ARTICLE INFO

Article history:
Received 9 February 2017
Received in revised form 28 April 2017
Accepted 24 July 2017

Keywords:
Automated HAZOP analysis
Fault tree synthesis
Hazard identification completeness
HAZOP quality
Formal languages
Alarm analysis

ABSTRACT

Hazard and operability analysis (HAZOP) has developed from a tentative approach to hazard identification for process plants in the early 1970s to an almost universally accepted approach today, and a central technique of safety engineering. Techniques for automated HAZOP analysis were developed in the 1970s, but still have not displaced expensive manual approaches. Reasons for this were investigated and conclusions are drawn. The author's actual experience in applying automated HAZOP techniques over a period of more than 30 years is revisited, including results from several full-scale validation studies and many industrial applications. Automated techniques, when combined with manual approaches, were found to provide significant improvements in HAZOP quality and a limited but valuable improvement in efficiency.

1. Introduction

Techniques for automated HAZOP analysis were described actually before the concept of HAZOP was openly published. Fussell (1973) described automated fault tree analysis by piecing together "mini fault trees", which provides a methodology for filling out the cause columns of a HAZOP table. Taylor (1975) and Taylor and Hollo (1977) presented algorithms for automated cause consequence analysis and fault tree analysis, together with a systematic approach to component modelling. Powers and Tompkins (1974a, 1974b), Powers and Lapp (1976) and Lapp and Powers (1977a, 1977b) published methods for fault tree analysis of chemical plant using signal directed graphs (digraphs), and Salem et al. (1975, 1977, 1979) and Salem and Apostolakis (1980) described the use of decision tables to support fault tree construction. Andow (1973) used functional equations as a representation for disturbance propagation in alarm analysis. Martin-Solis et al. (1977) and Poucet (1983) used logical equations to represent alternative causes of disturbances. Digraph models have similar power to mini-fault tree and state table approaches, but require preparation of a digraph form the process diagram such as a P&ID (Cui et al. introduced a method to make this transformation automatically.

The RIKKE program, developed by the author and J.V. Olsen using Fussel's mini-fault tree approach, was extended to cover feed forward and feedback loops. It was developed and validated by the expedient of helping to build a chemical plant, comparing the automated results with several manual analyses, and by assisting in the commissioning and operation (Taylor, 1982a, 1982b; Taylor and Olsen, 1983; Haastrup et al., 1985).

Since then there have been many doctoral theses and journal articles describing automated fault tree and HAZOP analysis methods. Yet there are still very few industrial applications of automated HAZOP, and companies still invest tens to hundreds of thousands of dollars in performing HAZOP manually in HAZOP workshops. Even worse, the manually completed HAZOPs are known to be incomplete (see e.g. Taylor, 2012). What went wrong? This paper discusses the development of manual and automated HAZOP over a period of forty years, reasons for the lack of success of automated HAZOP and reasons for the successes.

2. Obstacles to automated HAZOP

One of the first obstacles to the use of automated is the need to translate system drawings such as piping and instrumentation diagrams (P&IDs) into a special format. These can be either a simplified version of the P&IDs themselves or a more complex derived representations such as digraphs (e.g. Powers and Lapp, 1976) or multi level flow diagrams (Öhman, 1999). These derived representations proved to be complex and error prone for large systems, and often more costly than the manual HAZOP itself. This problem has been solved in recent years

E-mail address: roberttayloritsa@gmail.com

http://dx.doi.org/10.1016/j.psep.2017.07.023

by the development of software that can take commercial CAD drawings and translate them into “intelligent” drawings which can be used in accident simulation (Rossing et al., 2010). Cui et al. (2008, 2010) developed a system which could take in a CD piping and instrumentation drawing, convert it in a standardised way to digraphs, and use these for HAZOP. It should be noted that full commercial application requires not just translation of individual diagrams, but also integration of complete sets of diagrams.

Some P&IDs include the control signal flow paths, but in most cases safety and sequential control at least are described by means of cause and effects matrices, so that for a full analysis, these too must be integrated into the set of system drawings.

Some disturbance identified by HAZOP require quantitative judgements. An example from the plant shown in Fig. 6, and which actually occurred, is the possibility of a product freezing in a condenser, blocking the flow. This requires knowledge about the temperature of the condenser coolant, the rate of heat transfer from the product, and the product freezing point. In a fully automated analysis, such judgements need to be interpreted conservatively, which implies that the analyses need to be reviewed after completion, in order to reject those automated judgements which are incorrect.

Numerical judgements were found to be an issue in about 2% of the disturbances investigated in a total of 40 recent manual HAZOPS studied. Some researchers have incorporated numerical simulation into the automated HAZOP process so that judgements can be made automatically, but this requires a large additional effort unless a dynamic simulator is being constructed as a part of the design process. Even then the automated HAZOP software needs to be adapted to the specific simulator used (e.g. McCoy et al., 1999).

There are also issues of confidence and trust in the use of automated HAZOP. In modern practice the HAZOP workshop group has considerable authority and corresponding responsibility. Recommendations take on the role of formal and sometimes legal requirements, which must be implemented unless the designer can provide counter arguments. If a proposal is rejected then the designer is required to provide alternative solutions to the problem or a careful demonstration that the problem involved is a minor one. In order to be able to accept the responsibility for risk reduction recommendations the HAZOP team requires full understanding of the problems and the basis for analysis. This cannot be achieved via a purely computer generated HAZOP.

Another problem observed from study of accident reports is that there over 400 physical phenomena which have given rise to accidents in oil, gas and chemical plant (Taylor, 2014). The published automated methods have been observed to include up to about 30 of the most common of these. As an example, 13 different forms of liquid hammer were identified from accident reports, and liquid hammer was found to have caused 2% of the major accidents in refineries, yet these events could not even be represented in the formalisations used in first generation HAZOP methods. The automated methods based on disturbance propagation describe typically 23 phenomena. McCoy et al. (2000e) list 38 physical phenomena and in McCoy et al. (2000b) 14 phenomena related to loss of containment consequences. There does not appear to be any reason why this work could not be extended to cover all the known phenomena, but effort would be needed to ensure a practical level of discrimination.

A further problem was revealed by a study of ten high quality HAZOPS made from 2008 to 2014. About one third of the findings and recommendations from these were found to derive from drawing errors and detail design errors which are not related to process deviations and are not amenable to HAZOP analysis as described in guidelines. It is often said that such problems should be dealt with by a preliminary design review, but it was observed that many detail design problems can only be identified in the context of HAZOP. Examples are choice of material for a pipe, when the pipe can be accidentally subjected to low temperatures, or the decision about whether a valve should be locked open. The issue of automated design review is addressed below.

3. Completeness of analyses

A good HAZOP should preferably identify all significant accident consequences and the majority of accident causes, including all the cases which are likely to occur i.e. have a significant risk contribution. Under ideal conditions, completeness is defined as (Taylor, 1981):

$$\text{Absolute completeness} = \text{number of scenarios identified}/\text{number of possible scenarios}$$

Here scenarios are defined as an initiating event, a number of safety barrier failures and a consequence event. Completeness values depend on the degree of detail in the analysis, and all assessments here are predicated on the typical level of detail typical of professionally completed HAZOPS.

Completeness defined in this way has a problem in that the number of possible scenarios cannot be determined. Historical completeness is defined as:

$$\text{Historical completeness} = \text{number of scenarios identified}/\text{number of scenarios identified from an extensive incident database}$$

A database of over 1000 oil, gas and chemical industry accidents was developed to support completeness assessments.

A more valuable measure of completeness for hazard identification is to weight each accident scenario according to risk, but this can only be made practical if the HAZOP event frequencies and risk can be calculated easily (see third generation methods below).

For automated HAZOP, another important measure is discrimination, defined as:

$$\text{Discrimination} = \text{number of realistically possible scenarios}/\text{number of scenarios identified}$$

Without care in discrimination the HAZOP becomes useless. For example historical completeness could be ensured simply by incorporating all the scenarios from the database (leaving the analyst with the task of reviewing the automated analysis and discarding most of it). On the other hand fully automated analyses must compromise on discrimination because they must ensure that all scenarios which are in principle possible must be included, and the basis for inclusion may be uncertain. For example sump tank rupture due