Reliability Engineering and System Safety 108 (2012) 56–64

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

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

HASILT: An intelligent software platform for HAZOP, LOPA, SRS and SIL verification

Lin Cui [a], Yidan Shu [a], Zhaohui Wang [b], Jinsong Zhao [a,*], Tong Qiu [a], Wenyong Sun [b], Zhenqiang Wei [b]

[a] Chemical Process Accident Prevention and Emergency Research Center, Department of Chemical Engineering, Tsinghua University, Beijing 100084, China
[b] CNPC Research Institute of Safety & Environment Technology, Beijing, 100083 China

ARTICLE INFO

Article history:
Received 28 June 2011
Received in revised form
9 June 2012
Accepted 18 June 2012
Available online 26 June 2012

Keywords:
HAZOP
LOPA
Safety requirements specification
SIL validation
Knowledge management
PSM

ABSTRACT

Incomplete process hazard analysis (PHA) and poor knowledge management have been two major reasons that have caused numerous lamentable disasters in the chemical process industry (CPI). To improve PHA quality, a new integration framework that combines HAZOP, layer of protection analysis (LOPA), safety requirements specification (SRS) and safety integrity level (SIL) validation is proposed in this paper. To facilitate the integrated work flow and improve the relevant knowledge management, an intelligent software platform named HASILT has been developed by our research team. Its key components and functions are described in this paper. Furthermore, since the platform keeps all history data in a central case base and case-based reasoning is used to automatically retrieve similar old cases for helping resolve new problems, a recall opportunity is created to reduce information loss which has been cited many times as a common root cause in investigations of accidents.

1. Introduction

With the rapidly increasing scale and complexity of the modern CPI, it is becoming harder to control chemical accidents in chemical plants. Offsite consequences often lead to ecological disasters. For example, about 40% of large-scale environmental emergency events reported to the Ministry of Environmental Protection of China were caused by accidents occurred inside chemical plants. To prevent major accidents from occurring, the process safety management (PSM) programs have been implemented by many companies around the world since the PSM of Highly Hazardous Chemical standard, 29CFR 1910.119 was promulgated by the US Occupational Safety and Health Administration (OSHA) in 1992. However, the implementation degrees vary from plant to plant. It is interesting to note that for most accidents, companies are cited for failure to comply with this standard and no companies are cited after an accident for having a good PSM program [1]. There were a total of 6578 citations of past 1227 OSHA PSM inspections from 1992 to 2006 [2]. Among all OSHA citation data, incomplete process hazard analysis (PHA) was one of the most frequently cited. According to the PSM regulation, the purpose of a PHA study is to review a process design to identify hazardous scenarios and ensure they are properly safeguarded. A complete PHA study for a process design is the final check to make sure that the design activities for the plant have not generated any new unacceptable risks.

PSM standards have been implemented for nearly 20 years. However, catastrophic accidents are still persistently occurring and there is not an obvious decline in process safety events. Through investigations of accidents of the last decade it can be found that their occurrence was not due to unknown physical or chemical process hazards. Why did they still happen? One of the major reasons is that lessons have not been learnt by all people, only by some [3]. It is a well known fact that corporations don't have memories but their employees do. When the employees leave, their knowledge generally goes away with them. A 2006 research report indicated that 50% of the process industry workforce would retire in the next 10 years and that there was a shortage of trained staff available to replace them [4]. Therefore, authors have developed HAZOPSuite not only for facilitating HAZOP meetings, but also for HAZOP knowledge management [5] that help knowledge transfer and reuse through the open and structured use of expert knowledge.

Motivated by the same thought, authors have developed HASILT for PHA knowledge management through a single open platform. Although Bingham and Goteti [6] recommended the integration of HAZOP, LOPA and SIL validation, a clearly described integration strategy is still not available, and the corresponding software is rarely reported in literature. Therefore a software that combines them as

* Corresponding author. Tel.: +86 10 62783109; fax: +86 10 62770304.
E-mail addresses: mr.cuilin@mail.tsinghua.edu.cn (L. Cui), shuyd@tom.com (Y. Shu), xjyx_wzh@petrochina.com.cn (Z. Wang), jinsongzhao@tsinghua.edu.cn (J. Zhao), qiutong@tsinghua.edu.cn (T. Qiu), wei-zhenqiang@cnpc.com.cn (W. Sun), wei-zhenqiang@cnpc.com.cn (Z. Wei).

0951-8320/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2012.06.014

Nomenclature

CBR	Case based reasoning
CPI	Chemical process industry
ESD	Emergency shutdown
ETA	Event tree analysis
FMEA	Failure modes and effects analysis
FT	Fault trees analysis
HASILT	Integrated intelligent software system developed by the authors
HAZOP	Hazard and operability
HAZOPSuite	The prototype software system of HASILT
IPL	Independent protection layer
LOPA	Layer of protection analysis
MSDS	Material safety datasheet
OSHA	US occupational safety and health administration
P&ID	Piping and instrument diagram
PetroHAZOP	The prototype software system of HAZOPSuite
PFD	Probability of failure on demand
PHA	Process hazard analysis
PSI	Process safety information
PSM	Process safety management
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumental system
SRS	Safety requirement specification

well as SRS is much needed to ease the integration work flow and realize knowledge management through information technology.

In this paper, the PHA methods and some related issues are presented in Section 2, the integration framework will be described in Section 3, and the software platform HASILT will be briefly introduced in Section 4. There is a case study in Section 5 demonstrating the effectiveness of the software platform. Conclusions will be drawn in Section 6.

2. The PHA methods and related issues

There are several PHA methods recommended in the OSHA's PSM standards, including hazard and operability (HAZOP) study, what-if/checklist analysis, fault trees analysis (FTA), failure modes and effects analysis (FMEA). Among them, the HAZOP study method has been recognized as a best PHA practice in the CPI because of its thorough and holistic analysis methodology.

HAZOP analysis assumes that hazards arise in a process plant due to deviations from design intents or from acceptable normal behaviors. It systematically and critically identifies all the possible causes and consequences of each hypothesized process deviation in a formal and systematic way. Its methodology was described in the book written by Kletz [7]. He also reviewed the HAZOP's history and its future developments [8]. The standard IEC61882 by International Electrotechnical Commission is the official application guidelines of HAZOP.

The PHA methods, such as HAZOP, can be used at any point in the life cycle of a process or a facility, but it is most frequently used during the design stage when the process flow diagram and the P&IDs are essentially complete, or after each modification. According to the OSHA PSM standards, PHA also should be thoroughly updated at least every 5 years for a facility without any process related change.

However, HAZOP is time consuming and effort consuming. It takes a HAZOP team consisting of 5 to 8 domain experts 1–8 weeks to complete the HAZOP analysis of a typical chemical process. For a large scale chemical process such as a one-million-ton-per-year ethylene plant which has more than two hundreds of P&IDs, it takes a much longer time according to the HAZOP duration estimation by Khan and Abbasi [9]. To identify all of the potential hazards in the process, the HAZOP analysis has to cover different operation stages including planned startup, normal operation, planned shutdown, unplanned shutdown and unplanned startup. However, not all of the stages are considered in HAZOP meetings, which often leads to incomplete PHA. For example, the BP Texas City refinery explosion accident in March, 2005 occurred during the isomerization unit startup of which the HAZOP analysis had not been done. Another factor that contributes to incomplete PHA is that even an experienced HAZOP team may be prone to overlook some potential hazards during the tedious and day-after-day HAZOP meetings of a large scale chemical process.

To lower the workload of the HAZOP team and improve HAZOP analysis quality, there has been a considerable motivation for more than two decades to develop intelligent systems for automating PHA of chemical plants since the end of 1980s, using various methodologies [10,11,12,13]. However, few of the intelligent systems have been widely accepted by the CPI. The authors developed an intelligent HAZOP software platform, currently named HAZOPSuite based on case-based reasoning and ontology [5]. Up to the day when the authors are drafting this paper, HAZOPSuite has been deployed and used in the Dushanzi refinery of China National Petroleum Corporation (CNPC) for more than four years, and HAZOP studies of more than 90 refinery and/or petrochemical processes have been done by using this software platform.

Even though HAZOP has been a successful practice of PHA in the CPI for about a half century, not all chemical companies have practiced it. There might be many contributing factors. One reason that the authors want to mention is that HAZOP study is essentially designed as a qualitative approach, and it is not uncommon that the HAZOP team quickly estimates risk ratings based on their experiences. Lacking of an efficient quantitative risk estimation algorithm available in HAZOP analysis has resulted in inconsistency and ambiguity. Therefore, management people often get frustrated when they need to make decisions based on the HAZOP results. About ten years ago, Dr. Trevor Kletz already warned of this tendency by stating that "all techniques tend to degrade as they become more widespread and there is concern that some companies that claim to carry out HAZOPs are undertaking little more than a perfunctory examination of the line diagrams" [14].

Therefore another better PHA practice has to be adopted. HAZOP study is only used to identify the hazardous scenarios while some other semi-quantitative or quantitative risk assessment methods and technologies are adopted to determine the risk levels of the hazards identified by HAZOP. Tens of such semi-quantitative/quantitative methods or technologies such as fault tree analysis (FTA), event tree analysis (ETA) and layer of process analysis (LOPA) have been developed during the past decades [15,16,17,18]. Among these technologies, LOPA is often the first approach taken in quantifying risk [19]. It typically uses order of magnitude, instead of specific data, for estimating initiating event frequency, and the likelihood of failure of independent protection layers (IPLs).The method's primary object is to determine whether the existing safeguards against a potential risk scenario are sufficient, and what additional protections should by applied if they are not enough [20]. As the needed additional protections can be SIS (safety instrumented system), it can also be used to determine the needed SIL (safety integrity level) of a SIS [21].