Software Systems in Implementation of Process Safety at Chemical Process Industry

Yew Kwang Hooi, Universiti Teknologi PETRONAS, Malaysia

M. Fadzil Hassan, Universiti Teknologi PETRONAS, Malaysia

Azmi M. Shariff, Universiti Teknologi PETRONAS, Malaysia

Hanida Abdul Aziz, Universiti Teknologi PETRONAS, Malaysia

Sujendran Suppiah, Petronas Penapisan (Melaka) Sdn Bhd, Malaysia

ABSTRACT

Software systems have been used in chemical industry process safety operation and design to improve its efficiency. This paper provides a brief review and analysis of the state of the art and impacts of software systems in process safety. A study was carried out by interviewing personnel in charge of process safety practices in the Malaysian chemical process industry and digging into literature of technology for process safety. This article explores the functional and operational characteristics of software systems for safety and attempts to categorize the software according to its level of impact in the management hierarchy. The study contributes to better understanding of the roles of Information Communication Technology in process safety, the future trends and possible gaps for research and development.

Keywords: Process Safety, Software Systems; Computer-Aided Plant Safety; Process Safety Management System; Chemical Process Industry.

INTRODUCTION

Software technology has helped improving the safety of many complex operations (Ralph Schneider, 2002; Zhou, Wiebe, & Chan, 2011). A few examples where human lives are entrusted to software systems are air traffic controller, nuclear power plants, high-speed railway scheduling and space missions.

This article pays a special tribute to the roles of software systems in safety of chemical processes that handle Highly Hazardous Chemicals (HHCs). HHCs are defined as chemicals which may be toxic, reactive, flammable or explosive. To limit the scope, only specialized software systems for process safety application are studied.

Accident can happen due to presence of both hazard and cause. Hazard is an inherent chemical or physical properties that has the potential to cause harm or damage to people, asset, environment and reputation (Daniel A. Crowl, 2002). The risk is higher in a complex facility (Hossam A. Gabbar, 2004). A cause is an event such as an equipment fault or an unsafe human act which causes a deviation. A deviation is a non-conformance to the expected flow of an operation. A deviation may lead to a series of latent failures and eventually causing the active failure, which will trigger the hazard leading to an accident (Mohd Shariff, 2011).

Removing the root cause will prevent onset of deviation(s), hence prevention of an accident. The Swiss Cheese model, see Figure 1, presents an idea of an accident as being the outcome of a chain of latent failures. Each latent failure is a red flag to deviation, hence back-tracking allows removal of the cause. Safeguards that prevent, detect, control and mitigate a major accident are depicted as cheese slices. The hole sizes on each slice represent degree of weaknesses of the safeguard due to poor compliance with performance standards. By minimizing the size of the holes, the chance of all pin-sized holes being lined up can be greatly reduced, and so is the chance of a major accident.(Kuusisto, 2000)

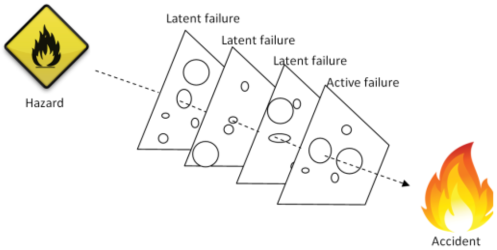

Figure 1. Swiss Cheese accident model. (B. Knegtering, 2009)

The goal of process safety in regards to process hazard is to minimize risk to As Low As Reasonably Possible (ALARP). Process safety requires detailed analysis and effective management of process hazards and causes (Zhao, 2005). Process safety involves, for instance, the prevention of leaks, spills, over-pressures, over-temperatures, corrosion, metal fatigue and other potential failures.

Two approaches to mitigate risk in process safety, according to (Daniel A. Crowl, 2002), are inherent safety and safety controls. Inherent safety, or safety by design, makes a process robust towards errors or abnormal operating conditions through process design (Mason, 2001). Safety control places measures to detect and react to deviations in order to reduce the risk.

Process safety is complex because of various reasons. Detecting root cause is difficult because latent failures, which are actually symptoms, can be mistaken as the root cause. Analysis by an expert to find the root cause is knowledge-intensive and often requires years of experience and proper tools (i.e. FTA, Fishbone, tripod beta, etc).

Software systems have been used to automate many of the industry's business processes including process safety. Surprisingly, (Ralph Schneider, 2002) quoted that very few literature is dedicated to explaining the roles of Information Communication Technology (ICT) in process engineering through an integrated view. However, many experts believe the significant role that computer systems can play in improving process safety (C. Palmer, 2008; Chung, 2003; Chunhua Zhao, 2003; Early, 2006; Elliott, 1994; Ghawi, 2010; Katalin M. Hangos, 2008; Lin Cui, 2010; Y. Naka, et al. , 2000; U. Hauptmanns, 1998; Zhao, 2005).

This article covers the different categories of software used in process safety and evaluate the impacts to the industry. The early sections explore the nature of the process safety industry. Various categorization criteria are established and compared with typical Information Systems and tools used in the industry. Functions and operational features are evaluated. Significance and contributions of this study to the body of knowledge and industry are elaborated in the analysis section. Finally, the trends of future development in process safety through the eyeglass of software system is expounded.

METHODOLOGY

Pragmatism paradigm using interpretive approach is used to conduct the study the environment. A series of interviews with experts and field observations are conducted. A dozen experts and experienced (5 years and beyond) field personnel from Safety Group and operations from 4 Malaysian HHC-processing premises were interviewed. The premises are chosen because implementing safety program is a major concern and the management has looked into various implementation approaches, including computer technologies. The premise includes a research pilot plant and full-scale operating plants. Selection criteria include that the plants handle HHCs and that ICT is used intensively in plant as part of the process safety activities. Field visits and on-site observations provide opportunities on how information is produced, communicated, used and stored.

To gain the macro view, literature on process safety software systems and technology are reviewed. Peer-reviewed literature from databases and publications such as EBSCO Host, Elservier, ISI Web of Science, SCOPUS, SpringerLink and process safety journals were read to search for experience sharing of process safety activities that involve the use of computer. The keywords are "Process Safety Management", "Process Safety Automation", "Information Technology AND Process Safety", "Computerization AND Process Safety", "Information System AND Process Safety", "Process Automation" and "Process AND Computer". Literature findings were verified and elaborated through interviews and discussions with domain experts and practitioners.

Findings are presented in concept matrices and discussion. Concept matrix was used to address the width of the study to depict relationships between ideas (Schuldt, 2005) and to keep the focus narrow (Rembrandt Klopper). The categories are determined by mapping the systems' functions to the hierarchies in a plant management pyramid. The categories of systems are differentiated by functional and non-functional attributes identified from the interpretive study. The findings are verified using positivism approach.

LITERATURE REVIEW

Process Safety Program

Process safety program is a set of activities concerned with design and engineering of facilities, maintenance of equipment, management of effective alarms, effective control points, updates of procedures and training throughout the life cycle of a chemical process plant. The life cycle begins with design of a process, procurement of equipments and instruments, operation (that includes maintenance and management of changes) and safe disposal (Hossam A. Gabbar, 2004).

Various aspects of plant safety is outlined in safety standards established through years of experience and research by the industry and academics. OSHA Process Safety Management (PSM) is a widely used standard for identification, prioritization and control of risk on people, facilities and the environment (Bingham, 2008; Mason, 2001; Mohd Shariff, 2011). It is a performance-based standard which clarifies "WHAT-TO-DO". The guidelines contains 14 perspectives of safety management which covers safety aspects at infrastructure level, operational level and design level.

Implementation deals with “HOW-TO-DO” and makes use of resources:-knowledge, technology, budget to achieve the goals set by the guideline. PSM implementation includes development of in-house competency; meaningful KPI and matrices for record and tracking. The implementation aspect is left to the plant management and subjected to cultural adaptations and available expertise to deliver the how-to (Christopher Cunio, 2013). Many plant operators implement their own flavour of PSM by incorporating the guidelines into existing risk and quality management (Morris Kho Kee Wee, 2008). Implementation of PSM is crucial to successful prevention of major accidents (J.F. Louvar, 2011).

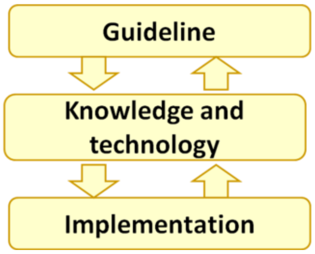

*Figure 2.*Implementation of process safety management guideline

See Figure 2, knowledge specific to a plant such as configuration and technologies are necessary ingredients of the implementation plan. There are many practical issues that requires commitment of resources from management to operation (Kaszniak, 2010).

There are very limited resources on PSM implementation. The US National Institute of Occupational Safety and Health (NIOSH), IChemE, Mary Kay 'O Conner, Center for Chemical PS and DNV Lloyd are focusing mostly on awareness level and services for specific areas such as hazards identification and risk assessment.

Full compliance to PSM could prevent accidents such as fires, explosions, releases of hazardous substances if process plants follow the regulation as intended (Josph F Louvar, 2008). Implementing PSM in many countries is due to directive from government or voluntary consensus program. (H.A. Aziz, 2014; Mohd Shariff, 2011). In Malaysia, PSM is not yet made compulsory but HHC process plant activities are controlled by CIMAH 1996

Process Safety Information

Process Safety Information (PSI) 29 CFR 1910.119(d)'s is one of PSM aspects that guides plant management to provide a complete, accurate and updated compilation of written process safety information on chemicals, technology and equipment (H.A. Aziz, 2014). Examples include block flow diagrams, process flow diagrams, process chemistry and process limitations (temperatures, pressures, flows, compositions)(Daniel A. Crowl, 2002). The compilation is accessible by all employees (Daniel A. Crowl, 2002), contractors and enforcement officials . The information is used to enhance other process safety matters (Safety/AIChE, 2011), which includes Process Hazard Analysis (PHA), development of training program, development of operating procedure, planning of local emergency preparedness, pres-startup review, management of change and investigation of accidents (Daniel A. Crowl, 2002). However, compilation was frequently cited incomplete in many facilities (Sutton, 2010).

Process Safety Work Flow

A workflow is an orchestrated pattern of organizational activities that processes work (transform materials, provide services, or process information) by passing it from one process to another. A process safety workflow requires a systematic input of resources (expertise, knowledge, information and data) into processes to produce analysis and recommendations of process safety.

A typical workflow is document-oriented (Misander, 2000) which generates documents (or product data) such as equipment data sheets, flow sheets (PFD, P&ID) and specification reports. This information may be shared by different workflows (Ralph Schneider, 2002) (Yahia, Aubry, Herv, #233, & Panetto, 2012). Since different workflows may be implemented by different parties in different systems or environments (Hossam A. Gabbar, 2004), a framework for coordinating collection and dissemination of comprehensive and timely information is necessary.

Process Safety Software Systems

The role of software to facilitate process safety is undeniable, as evidenced by computerized consoles in control rooms of any modern plant. The general functions of software is to monitor data and to allow operators to control equipments remotely through a digital interface. Hence, a large chemical complex can be manned by a small staff of operating personnel.

Generally, software systems enhance process safety through automation or semi-automation of manual processes such as capturing, storing, processing and communicating information. Higher productivity can be achieved through faster and reliable access, faster processing based on rules, visualization and better understanding through computer-aided modelling in process design (Perkins, 1996; Ponton, 1995; Ralph Schneider, 2002) and artificial intelligence to emulate human problem solving or decision-making. Additionally, software enables integration of more data or information sources, better representation of knowledge and higher rate of reuse of resources (Hossam A. Gabbar, 2004).

RESEARCH OBJECTIVE

From the perspective of information management, process safety is a complex domain with many pieces of information and corresponding applications that affect different tiers of the plant enterprise. The current literature does not provide an overall picture of the process safety software and how the applications can be categorized with clear distinction of roles. Consequently, this study aims to investigate the functional categories and the state of the art of software system in process safety.

The investigation provides justifications of the categorization based on empirical grounds and the insights that can be gained from such categorization in order to improve management of the domain information.

ANALYSIS AND DISCUSSION

Process safety requires specialized software. The categories, based on this study, are Process Control Systems (PCS), Safety Management Systems (SMS), Safety Method Tools (SMT) and repository systems, see Figure 3. Repository is a large collection of files which include database, images, videos, audios or documents stored in a proprietary software system (such as Content Management System) or a network drive.

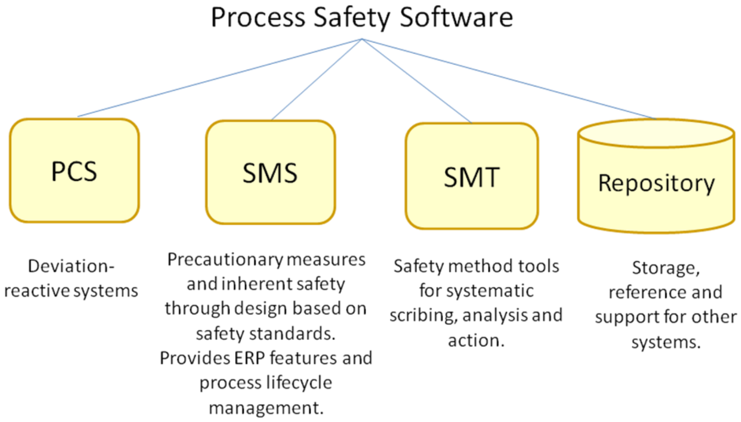
Process Safety Software
PCS
SMS
SMT
Repository
Deviation-reactive systems
Precautionary measures and inherent safety through design based on safety standards. Provides ERP features and process lifecycle management.
Safety method tools for systematic scribing, analysis and action.
Storage, reference and support for other systems.

Figure 3. Major categories of process safety software.

Process Control System (PCS)

PCS provides monitoring and control on top of existing process design. Sensors measure performance data such as temperature, pressure and volume. Controller compares the data with a certain reference and computes the necessary adjustment. Sub-categories of PCS are Basic Process Control System (BPCS), Advanced Process Control System (APCS), Safety Instrumented System (SIS), Programmable Logic Controller (PLC) and Supervisory System (SS).

BPCS is a Distributed Control System (DCS) that collects data from the field in real-time. The data is stored, used for basic process control or for advanced control. Operators use the data to perform basic controls such as PID controls, ratio controls and dynamic compensation. APCS extends BPCS by focusing on process optimization to improve economics of production..

SIS, a critical control system, is more specialized than BPCS. SIS provides an independent control system dedicated to fail-safe critical equipments. It helps critical process systems revert to safe states automatically when an unsafe condition occurs.

Programmable Logic Controller (PLC) provides a more basic control of system components than a BPCS. It is a computer monitoring and control system that continuously makes automatic decisions to control process equipments.

SS or better known as Supervisory Control, Data Acquisition and Processing (SCADA), is a PCS optimized for supervisory with minimal control capabilities. It couples with PLCs to provide visualization of a process through a Human-Machine Interface (HMI), see Table 1. It can be used to verify safety and control PLC by sending set-points that trigger safety alarms and interlocks. Specialized systems such as Fire and Gas Systems (F&G), Emergency Shutdown Systems (ESD) and Burner Management System (BMS) are a type of SS.

Although BPCS, APCS, SIS, SS and PLC share many structural similarities, distinction can be made by knowing the objective of each software system.

Table 1

Supervisory Systems(Daniel A. Crowl, 2002)

System	Description
SCADA	• Gather data and log events remotely. • Activate alarms when conditions become dangerous.

System	Description
	- Control equipment and conditions of PLC.
HMI	- An interface for communication or control of PLC.

Safety Management System (SMS)

SMS is an information system that supports PSM. It is used to manage process safety activities that lead to proactive creation, prevention and maintenance of a robust process safety through inherent design(Mohd Shariff, 2011). SMS contains a set of proactive and integrated policies, programs and procedures to formally define and manage safety risk. The goals of safety management, according to Kuusisto (Kuusisto, 2000), are to improve accessibility to process safety management documents by employees; to improve safety compliance through employer commitment; and to improve readiness for audit.

SMS is based on widely accepted guidelines such as OSHA Process Safety Management (PSM). SMS benefits PSM implementation by addressing challenges due to substantial time and resources requirement (Early, 2006). It enhances communication by providing data, information and services to many users in one or more organizations using synergy of technology and people (Hossam A. Gabbar, 2004). Table 2 summarizes computer-based efforts to streamline PSM implementation issues based on observations and interviews conducted.

Table 2

Software Strategy to Address Several Process Safety Management Issues

Issues	**ICT Strategy**
Mechanical integrity requires frequent assessment review, inspection and testing.	Web portal that provides workflow control, document repository and collaboration tools.
Large number of operating procedure (OP), outdated OP and manpower to maintain OP.	Centralized storage and content management for OP documents.
PHA workshop is long and maintaining commitment is challenging, plus attrition causes loss of ground experience.	Provide registers for hazard and effect; and software that supports consequence modeling, adequacy review, hazard review, revalidation and mapping study.
Regular and costly trainings.	Web-based training and certification for staff.
Changes are not properly communicated due to attrition, poor handover or missing documents.	Standardized online form. Document management system for centralized storage and versioning.

Incomplete or poorly managed PSI documents.	Checklist and document management system for gap analysis, versioning and ability to flag inaccuracy.
Process safety audits are not properly managed, tracked and closed	Web portal that manages the audits, tracks the action items and reports on the closure of the action item.

SMS is designed with a robust framework supported by models based on safety management guidelines such as PSM (Hossam A. Gabbar, 2004). A robust framework is required to model plant safety and its objects. Gabbar and Suzuki (Hossam A. Gabbar, 2004) proposes a set of frameworks as a backbone of SMS for OSHA PSM, see Table 3. PEEE facilitates the construction of models representing plant activities, diagrams, processes, safety-related entities and characteristics of a SMS. Safety objects (alarms, sensors, operating procedures) are mapped to elements of the models and used to monitor safety events.

Table 3
Safety Management Frameworks (Hossam A. Gabbar, 2004)

System Framework	Description
Plant Enterprise Engineering Environment (PEEE)	Provides standard and systematic model formalization method. Provides models and elements representing activities in a plant lifecycle.
CAPE-SAFE	Automated tools to manage plant safety lifecycle.
Specification of integration	Integrate both PEEE and CAPE-SAFE for exchange and sharing of life cycle information.

The Plant Lifecycle Model is used to analyze and understand the activities within a plant lifecycle. It contains sub-models "process model", "plant operation model" and "plant behaviour model". Plant model is a static model based on Process and Instrumentation Diagram (P&ID) to understand components of a plant as a topology of Control Group Units (CGUs) and the components. Plant operation model provides information of each equipment as a class method. Plant behavior model describes different states of a plant process and their transitions.

Plant safety mode provides information on safety within each model element of P&ID throughout the whole plant life cycle. A plant safety model is composed of multiple collaborating safety objects which are integrated into the plant lifecycle and main functional areas (design, construction, operation, maintenance, financial, human resource and procurement).

Safety Method Tool (SMT)

Safety Method Tool (SMT) refers to individual software developed to carry out a specific task in process safety. SMT provides further analysis on data set and documents from systems, individuals or groups to identify deviation, risk and root causes. Design engineers use the software to identify design weaknesses and to choose better alternatives.

For example, in Process Hazard Analysis (PHA), determining hazards is based on record or experience, the likelihoods are based on analytical approach and the impacts are based on intuition and judgment (Bradshaw, 2012). Hazard evaluation is an analytical information of direct, root and systemic causes using site-specific guidelines and appropriate method based on incident condition. (Rick Vaughan, 1998). Since PHA can be costly and very time-consuming, automation or semi-automation through SMTs can provide cost-savings and efficiency. SMTs often offer various methods:- Hazard and Operability Review (HAZOP), Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). Furthermore, SMT can help with registering findings and evidences of safe working environments and practices (Jeffrey Hahn, 2005) for reporting (Iris Karvonen, 1987).

Repository

Documents such as text documents, postscript documents, spreadsheet and HTML pages are kept in a file repository. Enterprise Content Management System or Enterprise Data Management System (EDMS) contains repository of managed documents at its core. As a software system, it provides value-adding service such as compliance-checking, archiving, a unified environment and web accessibility. Examples include FileNet and Documentum.

Documents, unlike database, are less structured for computer processing. Often, documents are kept by individuals hence an obstacle to effective sharing of knowledge of process safety. On the other end, documents stored in a repository may be outdated or orphaned over the time. Revising and organizing the documents are extremely challenging due to large number .

Database provides various advantages. Firstly, database server provides centralized service for different applications. Secondly, database is computer processable, as long as the software understands the schema of the data. A site database will become more meaningful with many years of capture of major incidents. Software analyzes a large collection of historical data to discover relationships and patterns of events leading to accident event. For example, the Process Safety Incident Database (PSID) is a database to collect, consolidate and share high learning value process safety incidents from participating companies to promote learning from incidents. Similarity between operation and one that experienced a loss is a clue for further actions. (Rick Vaughan, 1998). However, huge databases of many years are often littered with noises, i.e. bad data (data in wrong format or of an insensible value).

Knowledge Base

Knowledge base (KBS) is necessary in model-driven SMS to represent domain facts. Often, knowledge base is developed from scratch using existing data files and communications between experts. (Mike Uschold, 1995) speaks of the importance of knowledge base as the integration framework especially in a huge organization in order to reduce integration complexity.

Ontology is the prevailing model for knowledge base. It organizes concepts, properties and relationships in a graph-like structure. In process safety, ontology becomes references for both software systems and personnel for safety terminology and definitions to resolve semantics and conflicts of different terms used in different process workflows (Chunhua Zhao, 2003). A standard ontology for process engineering OntoCAPE contains a general process model (Marquardt, Morbach, Wiesner, & Yang, 2010) that can be extended to support SMS.

EVALUATION OF PROCESS SAFETY SOFTWARE

Safety software shares parallel functions of generic Information System (IS), except that the former's operation is driven by safety domain models. As with generic IS such as Transaction Processing System (TPS), Operation Automation System (OAS), Knowledge Work System (KWS), Management Information System (MIS) and Decision Support System (DSS), safety software provides capabilities such as data management, knowledge management, information retrieval, automation of common tasks and framework support for decision-making. Our findings are summarized in Figure 4 which displays software categories in both generic business IS and software systems mapped to the four-level pyramid model.

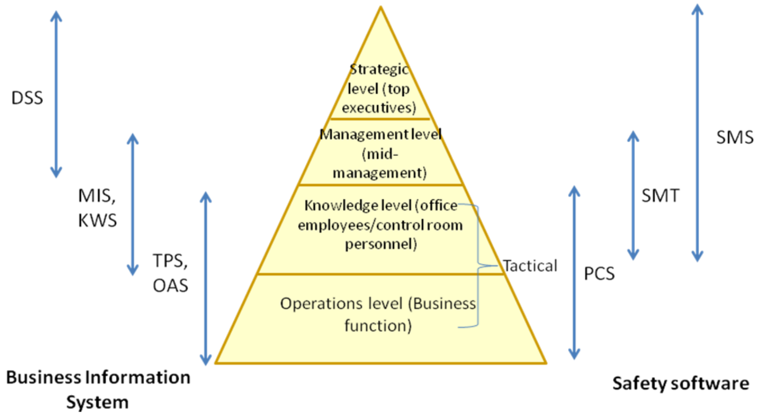
DSS
MIS, KWS
TPS, OAS
Strategic level (top executives)
Management level (mid-management)
Knowledge level (office employees/control room personnel)
Operations level (Business function)
Tactical
PCS
SMT
SMS
Business Information System
Safety software

Figure 4. Safety software used in different management hierarchy layers.

From the perspective of process safety, operation level includes routine safety inspection, tagging and other ground level works. Any near-misses or abnormal events are logged into a database by PCS. At knowledge level, personnel at the control room identify actionable information, e.g. a new deviation, from analyzing data fed by PCS. Then, an appropriate risk mitigation tactics can be carried out immediately. At strategic and mid-management levels, SMS and SMT are used to monitor performance, identify risk and plan an appropriate mitigation.

Figure 5 depicts two layers of activities in a plant:-operation and management. Operation refers to the ground works that involve direct contact with the equipments and process facilities. Management refers to planning and implementation of programs that ensure compliance with standard safety practices. This includes training, certification, permit, audit just to name a few. The block diagram of key safety software systems are deliberately placed within or between one of these two layers to illustrate the layers these systems operate in. PCS provides services for the operation layer. SMS, SMT and repository are placed on both layers, indicating the systems are likely used by users in both layers. SMS conceptual block takes up more space on the management, indicating its higher likelihood to be used by the management.

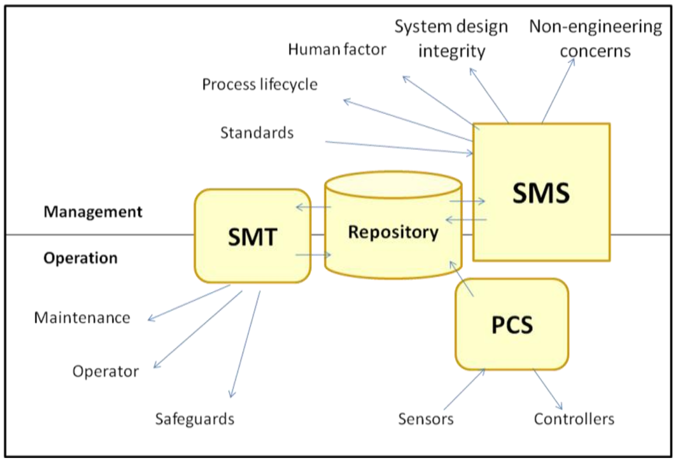

Figure 5. Relationship between different categories of safety systems.

A possible deployment of safety systems are illustrated in Figure 6. PCS resides in its own network setup for the plant and the control room. The corporate network is a separate physical network where SMS resides. SMT may be used on ad hoc basis in either PCS network, corporate network or both.

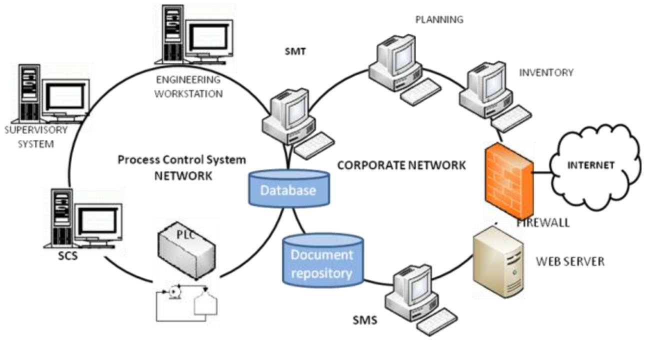

Figure 6. Deployment of process safety software systems. (Adapted from (Jeffrey Hahn, 2005))

Table 4 summarizes the functional features and operational features of process safety software. Functional feature refers to the roles that the system or its components are designed for, the set of inputs, the behaviour of the system and the set of outputs. Functional features are supported by operational features which describe the qualities of system.

Table 4

Functional Features of Process Safety Software

IS	**Monitor**	**Control**	**Analyze**	**Integrate**	**Assurance**
PCS	X	X			
SMT			X		X
SMS	X		X	X	X

Both PCS and SMS are used to monitor different levels of safety. PCS monitors the health status of equipment used in a process. SMS is used to ensure and verify that safety programs are carried out as per safety guideline. SMT is used to aid SMS by providing detailed analysis using established engineering methods on ad-hoc basis. Integration and assurance features are expected requirements which will be discussed in depth in the following section.

Table 5

Operational Features of Process Safety Software

Criteria	PCS	SMT	SMS
Reactive/Proactive	Reactive	Both	Proactive
Real-time/Batch	Real-time	Batch	Batch
Model-driven/Data-driven	Mainly data-driven	Both	Model-driven
Automation level	Automatic	Semi	Semi

Table 5 provides a generalized operational features of PCS, SMT and SMS. PCS is a data-driven automatic system that reads performance parameter of equipments through sensors and triggers necessary response. SMS, on the other end, is model-driven. Due to abundant but scattered and even obscured information, a model based on safety domain drives the system to find and extract data and information of interest from existing documents and data sources. Therefore, SMS is a proactive system because it seeks to improve by providing workflow template and check list of compliance requirements. SMS requires much human inputs and interpretations, therefore the system is semi-automatic. Automation can be done only if there is an established procedure on an established set of information source, as in PCS. SMT is usually carried out on ad-hoc basis and often manually. However, there is a growing research to semi-automate it (Chung, 2003; Iris Karvonen, 1987; Lin Cui, 2010; Shibly Rahman, 2009).

ISSUES FOR FURTHER RESEARCH

Software in process safety are limited as there are very few ready-made products and expensive if to be developed in-house. Major issues in existing software are poor capabilities in integration, management of change and assurance of safety. (Marquardt et al., 2010) (Ralph Schneider, 2002)

Integration of Process Safety Systems

Integration of existing software is complex due to poor messaging standard and interfaces. A risk factor itself, a poorly integrated software hinders flow of information and becomes a barrier for operators to identify the big picture of a potential hazard. (Perrow, 1984)

Technologically, standards have been established to allow different subsystems and data sources to interoperate. Standard for the Exchange of Product model data (STEP) allows easy exchange of plant data among different systems and domains. Internet-based solution is currently adopted by most of the industries to overcome some integration limitations of middleware, CORBA, which has been used as a backbone to integrate different heterogeneous systems.

SMS is an enterprise-wide system that requires a higher level of integration and necessity to resolve incoherent engineering and business views. Integration enhances monitoring the progress of a design project, detection of inconsistencies in the design data, and uncovering incomplete design tasks, especially with relevance to safety.

Poor integration may hinder effective sharing between separate software tools as a coherent design support system. The system should integrate the distributed, collaborative and concurrent design process carried out by interdisciplinary teams in different groups or even organizations but to date, there is no satisfactory solution. (Marquardt et al., 2010) .

Integration is deterred by heterogeneity and volumes of data and information. Invariably, the sources of the information are documents generated in different workflows. The workflows can differ philosophically and merging engineering and non-engineering inputs which creates gaps between activities is unavoidable. For an example, the engineer who is responsible for the design of a plant can make better decisions by getting access to procurement data.

Management of Change

SMS requires sufficient measures to identify and contain any risk cropping out from any change in process. Expansions, modifications, attritions and change of contractors may compromise safety. Changes in environment should be monitored as it may change the parameter or cause a new indicator to surface. Change management requires a thorough review by the Subject Matter Expert (SME) to ensure the changes are correct. This is followed by a fast and effective distribution of knowledge and information to affected process safety perspectives. Continuous updates throughout a plant's life cycle is necessary due to changes of technology and other factors (Y. Naka, et al., 2007). For an example, a change in design may require reissue of new operating procedures and training of operators. Hence, new workflows are triggered and concurrent workflows may be necessary to prevent any delay or to prevent compromise of safety due to time constraint.

Assurance

Assurance is defined as what is being stated as accomplished has actually been accomplished (Linarez-Royce, 2006). This requires collection of evidences from existing data sources as feedbacks to an implemented recommendation. Assurance requires integration of workflow and management of change. Integration provides better access and retrieval of evidence from all possible sources. Management of change ensures the evidence collected is updated continuously.

Standard Knowledge Model for Safety

Model management and knowledgebase (KBS) can extend the capabilities of SMS as a DSS. Because of SMS heavy reliance on domain knowledge, a potential work in this area is to create ontology that captures useful knowledge from domain experts and techniques for reuse. Existing standard ontology, notably OntoCAPE, does not capture safety aspects of process engineering in sufficient depth to support SMS.

LIMITATIONS OF THE STUDY

As the number of plants with software implementation of its safety management is very limited in Malaysia, the authors have to make sure that the studied plants are sufficiently representative of other plants. This is determined by selection criteria in which the plants handle HHC in huge capacity (more than 10,000 pound HHC at any time), implement compliance with safety guidelines such as OSHA PSM and embrace computer support. The authors have done further study into the current trend and future innovation through cited literature but we acknowledge that there could be current developments which are not yet captured in literature. The work does not present any quantitative result due to small sample of study. The qualitative result however gives some hints about current and future developments and challenges for future study. Also, this article does not include human factor although it is the most important factor in any successful safety implementation.

CONCLUSION

This article is a visitation on software-based improvement of chemical process safety. Generally, software provides efficiency through faster processing, better network for sharing, remote sensing, remote control and automation of process. Software improves consistency by orchestrated work flow and structured inputs. In process safety, domain-specific software helps catching deviations, tracking progress of resolution, retrieval of evidence on safety and providing inputs for safety-centric decision support. The major categories of chemical process safety software are Process Control Systems (PCS), Safety Method Tools (SMT), Safety Management Systems (SMS) and repository systems. Repository systems, PCS and SMT are more established than SMS.

SMS provides framework and models for strategic management of inherently safe plant design and compliance with safety guidelines. Despite the significance of SMS, there is a very limited literature on the implementation. The fundamental issues in SMS implementation are integration, merging engineering and business inputs, poor management of change and lack of assurance of quality. The challenges can be addressed through a good PSM implementation and technological development in knowledge management.

Software cannot replace the acumen of a trained individual but can never-the-less be a valuable tool to complement decision making and processing of massive amount of information through its consistency and speed. By having the latest piece of information, software can aid a pivotal decision-making in process safety.

REFERENCES

B. Knegtering, H. J. P. (2009). Safety of the Process Industries in the 21st Century: A Changing Need of Process Safety Management for a Changing Industry. *Journal of Loss Prevention in Process Industry, 22*(2009), 162-168.

Bingham, K. (2008). Process Safety Management - The Elements of PSM. *Process West, June 2008*(51).

Bradshaw, B. (2012). Process Safety Management. http://web.ornl.gov/sci/aiche/presentations/ProcessSafetyManagement-BillBradshaw-March2012.pdf

C. Palmer, P. W. Ã. (2008). A computer tool for batch hazard and operability studies. *J. Loss Prev. Process Ind., 21*, 537-542.

Christopher Cunio, G. M. (2013). *A Guide to the Legal Framework of the PSM Standard for Engineers.* Paper presented at the 9th Global Congress on Process Safety, San Antonio, Texas.

Chung, P. (2003). Computer-aided Hazard Identification. *FG2 Seminar.* from www.epsc.org/data/files/PRISM/Computer-aided_HAZOP.ppt

Chunhua Zhao, M. B., Venkat Venkatasubramaniam. (2003). Roles of ontology in automated process safety analysis. *Computer Aided Chemical Engineering, 14*, 341-346.

Daniel A. Crowl, J. F. L. (2002). *Chemical Process Safety: Fundamentals with Applications* (2 ed.): Pearson Education International.

Early, W. F. (2006). Database management systems for process safety. *Journal of Hazardous Materials, 130*(1-2), 53-57. doi: 10.1016/j.jhazmat.2005.07.039

Elliott, M. S. (1994). Computer-Assisted Fault-Tree Construction Using A Knowledge-Based Approach. *IEEE Transaction on Reliability, 43*, 112-120. doi: 10.1109/24.285124

Ghawi, R. (2010). *Ontology-based Cooperation of Information Systems.* Universite De Bourgogne, Univ of Burgundy. Retrieved from http://hal.archives-ouvertes.fr/docs/00/55/90/89/PDF/these_A_GHAWI_Raji_2010.pdf

H.A. Aziz, A. M. S., R. Rusli, Yew Kwang Hooi. (2014). Managing process chemicals, technology and equipment information for pilot plant based on Process Safety Management standard. *Process Safety and Environment Protection, 92*(5), 423-429. doi: DOI: 10.1016/j.psep.2014.02.011

Hossam A. Gabbar, K. S. (2004). *The Design of a Practical Enterprise Safety Management System*: Kluwer Academic Publishers.

Iris Karvonen, J. S., Perttu Heino. (1987). *HAZOPEX - expert system supporting the safety analysi.* Paper presented at the SRE-symposium Helsingör, Denmark.

Jeffrey Hahn, D. P. G., Thomas Anderson. (2005). *Process Control Systems in the Chemical Industry: Safety vs. Security.* Paper presented at the 20th Annual CCPS International Conference.

Kaszniak, M. (2010). Oversights and Omissions in Process Hazard Analysis: Lessons Learned from CSB Investigations. *Process Safety Progress, 29*(3), 264–269.

Katalin M. Hangos, E. N., Rozalia Lakner. (2008). *A Procedure Ontology for Advanced Diagnosis of Process Systems*. Paper presented at the Proceedings of the 12th international conference on Knowledge-Based Intelligent Information and Engineering Systems, Part I, Zagreb, Croatia. http://link.springer.com/chapter/10.1007%2F978-3-540-85563-7_64

Kuusisto, A. (2000). *Safety Management Systems - Audit Tools and Reliabilities.* Technical Research Centre of Findland, Technical Research Centre of Finland.

Lin Cui, J. Z., Ruiqi Zhang. (2010). The Integration of HAZOP Expert System and Piping and Instrumentation Diagrams. *Process Safety and Environmental Protection, 88*(2010), 327-334.

Linarez-Royce, N. (2006). *Integrated Safety Management System (ISMS) Description.* (CPR400.1.2), Sandia Corporation (Sandia).

Louvar, J. F. (2008). Improving the effectiveness of process safety management in small companies. *Process Safety Progress, 27*(4), 280-283. doi: 10.1002/prs.10267

Louvar, J. F. (2011). How to Prevent Process Accidents. *Process Safety Progress, 30*(2), 188-190.

Marquardt, W., Morbach, J., Wiesner, A., & Yang, A. (2010). *OntoCAPE: A Re-Usable Ontology for Chemical Process Engineering*: Springer Publishing Company, Incorporated.

Mason, E. (2001). Elements of process safety management: Part 1. *Chemical Health & Safety, July/August 2001*.

Mike Uschold, M. K., South Bridge Rosanne House, Stuart Moralee, Yannis Zorgios. (1995). The Enterprise Ontology. *The Knowledge Engineering Review, 13*, 31-89.

Misander, P. (2000). A Document-oriented Model of the Workflow in an Engineering Project. *EU-Project CAPE.NET, TWG 4: Concurrent Process Engineering*. htp://capenet.chemeng.ucl.ac.uk

Mohd Shariff, A. a. A. A., Hanida and Roslan, Mohd Rafizie and Yew , Kwang Hooi (2011, 20th – 22nd Sept 2011). *Protecting live and business through best Process Safety Management practices.* Paper presented at the Proceedings of Asia Pacific HSE Forum in Oil & Gas & Petrochemicals, Fleming Gulf Conferences., Kuala Lumpur Malaysia.

Morris Kho Kee Wee, B. J. (2008, April 6-10, 2008). *Strengthening Process Safety Requirements in HSE Management System - an NOC's Experience.* Paper presented at the 2008 Spring Meeting & 4th Global Congress on Process Safety, New Orleans, LA.

Naka, Y., et al. (2007). *Information Model And Technological Information-Infrastructure For Plant Life Cycle Engineering.* Paper presented at the ICheaP-8 The eight International Conference on Chemical & Process Engineering.

Naka, Y., et al. . (2000). Technological information infrastructure for product lifecycle engineering. *Computers & Chemical Engineering, 24.*(2), 665-670.

Perkins, J., & Walsh, S. (1996). Optimization as a tool for dsign/control integration. *Computers & Chemical Engineering, 20*(4), 315-323.

Perrow. (1984). *Normal Accidents: Living with High Risk Technologies*. New York: : Basic Books.

Ponton, J. (1995). Process Systems Engineering: Halfway through the First Century. *Chemical Engineering Science, 50*(24), 4045-4059.

Ralph Schneider, W. M. (2002). Information Technology Support in the Chemical Process Design Life Cycle. *Chemical Engineering Science, 57*, 1763-1792.

Rembrandt Klopper, S. L., Hemduth Rugbeer. The Matrix Method of Literature Review. *Alternation, 14*(1), 262-276.

Rick Vaughan, B. K. (1998). *CCPS Process Safety Incident Database (PSID).* Paper presented at the Reliablity and risk management International conference, Reliablity and risk management.

Safety/AIChE, C. f. C. P. (2011). Guidelines for Auding Process Safety Management Systems, 2nd Edition., 39-61.

Schuldt, B. A. (2005). Concept Matrix Approach to Teaching Management Information Systems. *The Journal of Learning in Higher Education, 1*(1), 11-16.

Shibly Rahman, F. K., Brian Veitch, Paul Amyotte. (2009). ExpHAZOP: Knowledge-based Expert System to Conduct Automated HAZOP Analysis. *Journal of Loss Prevention in Process Industry, 22*(4), 361-554.

Sutton, I. S. (2010). Process Risk and Reliability Management - Operational Integrity Management. *Process Safety Progress, 29*(3), 273-274. doi: DOI: 10.1002/prs.10396

U. Hauptmanns, M. M., T. Knetsch. (1998). Computer-aided valuation of safety management. *Trans IChemE, 76*(4), 286-290. doi: 10.1205/095758298529641

Yahia, E., Aubry, A., Herv, #233, & Panetto. (2012). Formal measures for semantic interoperability assessment in cooperative enterprise information systems. *Comput. Ind., 63*(5), 443-457. doi: 10.1016/j.compind.2012.01.010

Zhao, C. H. V., V. (2005). *Learning in Intelligent Systems for Process Safety Analysis.* Paper presented at the European Symposium on Computer Aided Process Engineering -15, 38th European Symposium of the Working Party on Computer Aided Process Engineering.

Zhou, Q., Wiebe, A. J., & Chan, C. W. (2011). *Knowledge Engineering in the domain of Carbon Dioxide Capture Process System*. Paper presented at the SEKE. http://dblp.uni-trier.de/db/conf/seke/seke2011.html#ZhouWC11