Interoperation of Elements in Process Safety Management Via Ontology-oriented Architecture

Yew Kwang Hooi, Mohd Fadzil Hassan, Tan Xiao Ci
Universiti Teknologi PETRONAS,
Bandar Seri Iskandar, 31750 Perak, Malaysia

***Abstract*—This paper presents concepts of building a system using ontology to conduct risk identification in safety management of chemical processes. Manual risk identification requires laborious efforts in collecting and analyzing data for different process safety elements. Ontology provides intelligent integration of affected elements. Each element is represented by an ontology that provides future application with knowledge of process safety. In a distributed environment, each ontology can be represented by agent that exchanged the information to fulfill the requirement of the analysis.**

***Index Terms*—ontology, process safety management, hazard identification.**

I. Introduction

Process is a composition of equipments, materials and human actions to generate output at a desired rate; with acceptable quality, lifespan of process components; and without harm to both humans and environment. [1].

Inadequate safety review and management are significant factors of major accidents [2] [3] [4]. A process is a potential safety hazard especially if it is dealing with highly hazardous chemicals (HHC) such as explosive, flammable, corrosive or toxic materials or liquids.

Process Safety Management (PSM) standard, 29 CFR 1910.119 mandates a system safety approach to control hazards [5] and was developed specifically to address worker safety [6]. Other PSM systems include Risk-base Process Safety (RBPS), Chemical Process Safety (CCPS) 20 element guidelines and ACC's Process Safety Code ™ (PSC). PSM improves process technology [7], hence reducing industrial accidents [8] and operational errors [9].

A suitable PSM system or model is a life-cycle containing a set of proactive methods of a controlled safety management [10] [1] covering 14 Elements (details in Appendix 1 and 2): Employee participation; Process Safety Information; Process Hazard Analysis (PHA); Operating Procedures (OP); Training; Contractors; Pre-startup safety review; Mechanical integrity; Hot work permit; Management of change; Incident investigations; Emergency planning and response; Compliance audits; and Trade secrets

Integrating PSM elements into routine plant operations is a growing requirement. Plants rely on various document tools such as Major Industrial Accidents Council of Canada (MIACC) Self Assessment Tool to assess vulnerabilities in existing systems for control of major accident hazards [11].

II. Risk Identification

The purpose of risk identification is for prevention and mitigation of hazards in process safety. Events causing possible accidents, probabilities of occurrences and consequences are determined [12]. It requires knowledge of process, identification and analysis of risk and integration with start-up of a new or modified process.

Hazard identification is laborious and knowledge intensive. The techniques are usually laborious and expensive [13-15]. A successful identification requires sufficient input from field personal, updated documents/drawings and management support [16]. Factors such as motivation of the study, type of results needed, types of available information, characteristics of the analysis problem, perceived risk associated with the process and preference are evaluated [16].

III. Interoperability Problem

Using PSM, the identification addresses separate but interrelated elements. The elements are separate because it is easier and more practical to manage the elements separately in actual plant environment. The elements are interrelated because amendments done to one element may lead to amendments of another.

Many previous works have highlighted the technique to capture knowledge of human factor from the field. Very few studied the use of ontology for hazard evaluation in PSM, especially to integrate the PSM elements for risk identification [1].

Interoperability of elements, through mapping of each ontology is important and can be illustrated by human factor analysis. Existing PSM systems do not have an explicit human factor element. Risk-Based Process Safety (RBPS) contains human factor standard spread within its 6 PSM elements. In OSHA PSM, human factor is dimly mentioned in PHA, OP and Training elements. Hence, there is a need to make sure that human factors in the elements must work together in order to effectively address human errors [1].

IV. Human Errors

99% of accidental losses are due to human errors as a result of poor management. Human factor deficiencies include worker fatigue, poor human-system-interface design, poor communication, out-of-date and inaccurate operating procedures and poor communication between shift handover[1].

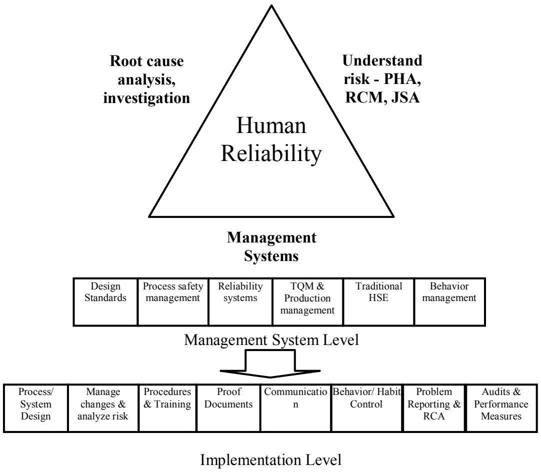

Figure 1. Controlling risk [16]

Risk identification is a part of human error risk control model proposed by Process Improvement Institute, see Fig. 1. Identification contains 2 out of the 3 facets of risk control activities:- analysis of root cause and understanding of the risk. Management systems control human error at management system level and implementation level.

V. OBJECTIVES

This paper presents the concept of a system that uses ontology to describe the taxonomy of individual PSM elements and to integrate the elements for human factor risk identification. A systematic framework is required to ensure a thorough and effective review for human factor through automated information exchange between ontologies. An example using human factor is discussed to illustrate the importance of interoperability between ontologies.

This work lays the foundation for future research and development for computer-automated PSM.

VI. RESEARCH BACKGROUND

A. Ontology

Ontology engineering is a systematic and formal conceptualization of a domain by defining individuals or classes of similar individuals and properties providing relationships between them [17].

Ontology, being a formal specification of a conceptualized domain of interest, permits computer reasoning. It is a promising technology to streamline system integration's process. Ontology helps with the development of intelligent system. Su et. al., proposes ontology for coping with dynamic OR environment. Technology can be used to reduce human errors and to improve safety, as stressed by several research papers. In medical domains, errors can be reduced by as much as 55%[18].

Taxonomy is a grouping of subsets in the domain based on common characteristics of each subset. The characteristics are specified by ontology. There may be more than one taxonomies for a domain, determined by chosen subsets of ontological characteristics.

Ontology is used to address issues: integration [19], reusability of knowledge, data sharing, interoperability, context awareness and semantic data mining [20].

Complex information exchange between concepts can be resolved through a better structured communication of knowledge and consensual understanding [21].

Context awareness is a research field in computer science seeking to deal with linking changes in the environment of computer systems. Context aware system can provide relevant services and information to user by exploiting context. The context of human factors are information on the user; user's social environment; and user's task. The context of physical environment are location; infrastructure; and physical condition (noise, light).

Users of ontologies are people, databases and applications that need to share a domain information. Ontology can be developed using Resource Description Framework (RDF) and Web Ontology Languages (OWL).OWL is designed for ontology-driven applications that need to process the content of information instead of just presenting information to humans. Sarker, Wallace and Gill (2008) have ranked top ontology tools: Protege, Altova and TobBraid Composer[22].

B. Hazard evaluation

TABLE I
HAZARD IDENTIFICATION METHODS

Method name	Description
Hazard and Operability (HAZOP)	a structured methodology for determining all possible deviations for a specific piece of equipment that can lead to hazard or operating consequences [12, 23].
Fault Tree Analysis (FTA)	Used extensively in process safety [24] to determine the possibility of an accidental event [7] using deductive reasoning to describe an accident model and to interpret the relationship between malfunctions of components or symptoms [25].
Checklist	a list of items and possible problems in the process to verify that various requirements have been fulfilled and nothing is neglected or overlooked [12].
Failure Mode, Effect and Criticality Analysis (FMECA)	tabulates a list of equipments in a process. The failure modes of each piece of equipment is determined and the impact on the system performance is evaluated [12].
What-if	asks a series of questions beginning with "What if ..." to identify potential hazards and solutions [12].
Human error analysis	identifies part of a process that has higher than average probability of human error [12].

There are several common methods to evaluate hazard, see Table 1 [26]. The methods provide a framework to detect possible deviations, probabilities of deviation and/or deductive reasoning that describes an accident model.

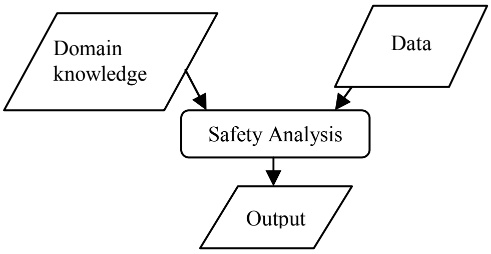

Figure 2. Context diagram of the proposed system framework

Intensive knowledge of safety domain and data is required to carry out an effective analysis, see Fig. 2. Domain knowledge may be a group of knowledge such as the chemical process, the methodology used to implement safety analysis, specific requirements by human factor analysis, etc. Data refers to configuration, people, date, threshold values, etc for a specific equipment/event at a specific time instance which is very specific and may differ from one plant to another.

C. *Computer support*

Computer support for safety analysis, is basic, mainly in the form of electronic reporting and data storage. Examples of automated HAZOP tools are LDG HAZOP [27], ExpHAZOP+, PHASuite, HAZID [13] and TOPHAZOP[26]. Typically, these tools use a list of deviations to identify possible faults for the analysis and rely on human decision heavily [27].

Chang and Yu have proposed an alternative to process analysis using Signed Directed Graph (SDG) as structured knowledge representation to diagnose faults in operating plants. The continuous process response of an operating plant is discretized into various smaller states of response for analysis of the variables using the truth tables. The proposal is interesting because it helps modularizing the fault to several smaller hence more manageable states of system response. SDG proposed is used for rule-based diagnostic system. Although enhanced by better methods, SDG is vulnerable to spurious and erroneous interpretation especially in a non-single transition [28].

A more advanced tool such as HAZID provides automated mapping of component icon in diagram to actual model and query facility for comparison of analysis results. For analysis, the system needs a knowledge base of equipments. Relationships between variables:- *faults*, *deviations* and *consequences* are established using arcs in knowledgebase. [13]

HAZOP expert systems can also be linked with Computer Aided Design (CAD) system. An ontology library and a new module could be developed to acquire data from CAD systems [27].

D. *Integration of knowledge for analysis*

Each element in PSM can be represented using an ontology. PSM element is often large and analysis often requires two or more elements. The entities of each ontology need to be mapped to one another so that a common framework can be used, hence allowing interoperability.

Several elements in PSM, i.e. PHA, OP and Training must work together in order to effectively address human errors. [1]. Since computer system is used, another PSM element, PSI becomes relevant. Table 2 provides explanation on the source of information and outcomes of the mentioned elements.

TABLE 2
PSM ELEMENTS FOR COMPUTERIZED INTEGRATION

Elements	Data source	Outcome
PSI	Manufacturer's Safety Data Sheet (MSDS), Process Technology Information, Employee participation	Need to establish consequences of deviation. Compiled for PHA. Relationships between safe operation and quality initiatives. PSI database.
PHA	Analysis techniques, previous cases, experts on hazard analysis method, experts on routine operations of a process	Documentation of lesson learnt in consequences, mitigation and control response; issue identification; and recommendation of correction.
OP	Standard procedures on safety precautions, normal routine, emergency start-up, turn-around and shutdown.	Updated, accurate and visible standard procedures.
Training	A planned schedule.	Implementation

VII. FRAMEWORK

This paper proposes the architecture of an application that is driven by ontology design for PHA addressing human factors. The system follows a structured flow, see Fig. 3.

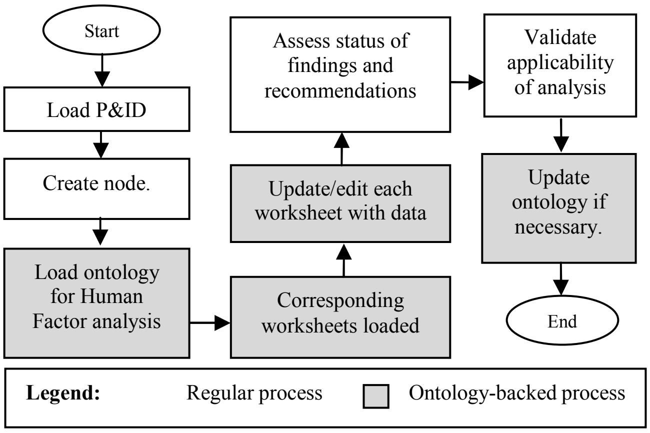
Start
Load P&ID
Create node.
Load ontology for Human Factor analysis
Corresponding worksheets loaded
Update/edit each worksheet with data
Assess status of findings and recommendations
Validate applicability of analysis
Update ontology if necessary.
End
Legend:
Regular process
Ontology-backed process

Figure 3. Process flow to conduct ontology-driven Human Factor analysis .

To begin, Process and Instrumentation Diagram (P&ID) is loaded into the application (see Figure 3). Process design is graphically depicted by Process and Instrumentation Diagram (PID). PID contains the layouts of the components used in a process and the relationships.

Instruments that are collectively evaluated are encircled in a boundary, called node. A PID may have one or more nodes. Each node contains PHA element of PSM. Human Factor analysis requires two other PSM elements :- OP and Training [1], hence integration is required.

Knowledge to conduct Human Factor (HF) analysis on the node is loaded by selecting OWL file from knowledge base. The ontology is referred by the application to load forms, i.e. worksheets needed to conduct HF analysis. The ontology determines the number and types of worksheets required, and the fields of each worksheet. In our example, HF analysis requires PSM elements such as PHA, OP, Training and PSI. Worksheets and workflow corresponding to the elements are loaded.

The content of the worksheets is updated by user based on review findings. As mentioned, some properties of the various elements are related. Hence, the ontologies of each element need to be mapped. HF ontology stores relationships between ontologies of various mentioned PSM elements. User enters data and the system updates the worksheets in multiple related locations. In case of collision with existing data, alert can be raised so that validity of the new or old data can be verified. Each worksheet may be using a common set of keywords. The keywords may be captured and reused through ontology.

Using the worksheets as guide, the management of the plant may follow up with progress of raised matters, recommendations, status of completion and other particulars such as person-in-charge and datelines. The ontology used may be revised and updated as necessary.

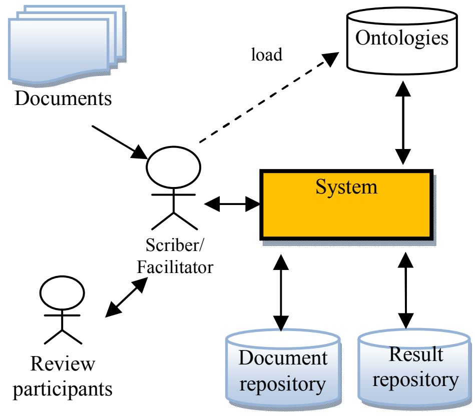

Figure 4. System architecture for ontology-driven PSM-compliant PHA.

Fig. 4 depicts the input of the system from review participants and documents such as P&ID and equipment specifications. The inputs are stored in result repository which are captured in the form of worksheets. The worksheets needed for the review are determined by the ontology used. The scriber makes use of the worksheet to guide the review and to capture the data required from participants and documents.

The system provides automation whereby overlapping areas of elements address HF are automatically addressed. Besides, ontology can be used to provide knowledge of the following:

a. Mapping of components on P&ID with knowledge base of the component.
b. Mapping of components with knowledge base of PSM elements.
c. Recovery of missing data.
d. Synchronized update of older data across different elements.
e. Relationships between hazards, deviations and consequences.
f. Utilization of equipment parameters:- reliabilities, probabilities of failure, failure rate, Mean Time Between Failures (MTBF).

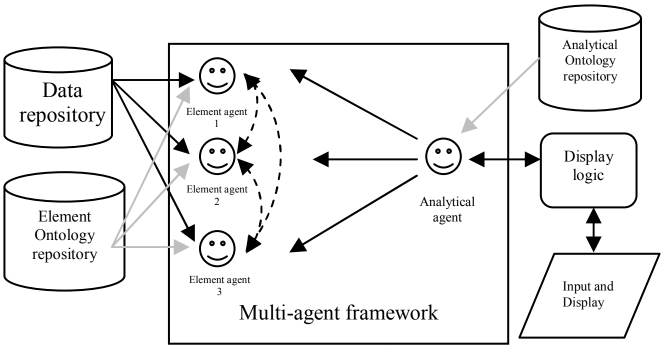

Figure 5. Components of the system

Multi-agent framework, for example JADE, is a framework for instantiation of agent objects, a hub for inter-agent communication and provider of shared services. See Fig. 5. Each agent is programmed to handle an ontology by providing abilities to find data from data repository, modification according to specification given by ontology and to communicate the changes with other agents. These agents are called "element agents" because they manage the data specific to an element.

Another agent provides services to translate and to map the ontologies. The analytical agent contains mapping algorithm and refers to an analytical ontology. The mapping algorithm resolves differences between target ontologies whereas the analytical ontology provides knowledge to manipulate other ontologies through their respective agents.

To illustrate how the above system can be applied to HF analysis, assume that the element agents are each managing an ontology for different PSM elements:- PHA, OP, Training and PSI. The analytical agent handles ontology of Human Factor analysis. Equipped with the knowledge provided by the ontology, the analytical agent seek element agents, coordinate them and update the result.

VIII. Discussion

Ontology provides intelligent integration of various PSM elements. Example of information that require integrations and synchronizations of the elements are:

a. update status
b. schedule, i.e. corresponding dates in different elements.
c. methodology for hazard identification
d. evidence, i.e. files.
e. person in charge.

An advantage of ontology-driven system is flexibility to change of knowledge. For example, HF analysis may change by adopting new methodology. Ontology may be modified accordingly by mapping HF ontology with a new ontology describing a new methodology. The system dealing with HF analysis does not need to be changed, hence reducing chances of system error and allowing changes to take place in a shorter period of time. Changes are accommodated by loading updated ontology.

However, the drawback of ontology is a heavy coupling between the system and the ontologies. Since some analysis requires more than one ontology, remapping of ontologies are required when a change occurs.

IX. Conclusion And Future Direction

The proposed system architecture of using multi-agent environment for coordination of ontologies for PSM system is novel. The application is ontology driven because the display system is affected by the data requirement specified for analytical agent. The analytical agent requires a specially designed ontology and mapping algorithm in order to function appropriately. Future work may include development of ontologies and mapping algorithm. Furthermore, there is a lack of proper technique to evaluate the quality and performance of ontology-driven system.

Acknowledgment

The authors would like to thank A. P. Dr. , Azmi M. Shariff and Puan Hanida Aziz of Process Safety Group, Universiti

Teknologi PETRONAS for rendering support and knowledge to this research and development.

REFERENCES

1. Bridges, T. *Human Factors Elements Missing from Process Safety Management (PSM)*. in *6th Global Congress on Process Safety*. 2010. Texas: American Institute of Chemcial Engineers.
2. OSHA, *Regulation Process Safety Management of Highly Hazardous Chemicals*. 1992.
3. U.S. Environmental Protection Agency (EPA) , U.S.O.S.a.H.A.O., *EPA/OSHA Joint Chemical Accident Investigation Report*. 1998.
4. (BP), B.P., *Deepwater Horizon Accident Investigation Report.* 2010.
5. Mason, E., *Elements of process safety management: Part 1*, in *Chemical Health & Safety, July/August 2001*. 2001, Elsevier Science Inc.
6. Dewolf, G.B., *Process safety management in the pipeline industry: parallels and differences between the pipeline integrity management (IMP) rule of the Office of Pipeline Safety and the PSM / RMP approach for process facilities.* Journal of Hazardous Materials, 2003. **104**: p. 169-192.
7. U. Hauptmanns, M.M., T. Knetsch, *Computer-aided valuation of safety management.* Trans IChemE, 1998. **76**.
8. Elliott, M.S., *Computer-Assisted Fault-Tree Construction Using A Knowledge-Based Approach.* IEEE Transaction on Reliability, 1994. **43**: p. 112-120.
9. U. Hauptmanns, M.M., T. Knetsch, *GAP -a fault-tree based methodology for analyzing occupational hazards.* J. Loss Prev. Process Ind., 2005. **18**: p. 107-113.
10. CH2MHILL. *Process Safety Management Compliance*. 2010 June 2011]; Available from: http://www.ch2m.com/corporate/services/industrial_safety/assets/process-safety-management.pdf.
11. Bingham, K., *Process Safety Management - The Elements of PSM.* Process West, 2008. **June 2008**(51).
12. Crowl, D.A. and J.F. Louva, *Chemical Process Safety: Fundamentals with Applications*. 1 ed. 1989, New Jersey: Prentice Hall.
13. Chung, P. *Computer-aided Hazard Identification*. FG2 Seminar 2003; Available from: www.epsc.org/data/files/PRISM/Computer-aided_HAZOP.ppt.
14. S. Viswanathan, N.S., V. Venkatasubramanian, *A hybrid strategy for batch process hazards analysis.* J. Computers & Chemical Engineering, 2000) **24**: p. 545-549.
15. Yet, P.I., *Development and applications of CASEHAT-A multipurpose computer aided hazard analysis automation system used in semiconductor manufacturing industry.* J. Loss Prev. Process Ind., 2003. **16**(271-279).
16. Bridges, W. *Selection of Hazard Evaluation Techniques*. 2011 15th December 2011]; Available from: http://www.process-improvement-institute.com/_downloads/Selection%20of%20Hazard%20Evaluation%20Techniques.pdf
17. Horridge, M., *A Practical Guide To Building OWL Ontologies Using Protégé 4 and CO-ODE Tools*, S. Brandt, Editor. 2011, The University Of Manchester: Manchester.
18. Chung-Jun Su, T.-Y.L., Chia-Wen Chih, *Toward Ontology Driven Context Aware Intelligent Operating Room*, in *The 11th Asia Pacific Industrial Engineering and Management Systems for Conference*. 2010: Melaka.
19. Uschold, M.a.R.J. *A Framework for Understanding and Classifying Ontology Applications*. in *IJCAI-99 Workshop on Ontologies and Problem-Solving Methods: Lessons Learned and Future Trends*. 1999. Stockholm, Sweden: CEUR Publications and University of Amsterdam.
20. Kuo, Y.-T., et al., *Domain ontology driven data mining: a medical case study*, in *Proceedings of the 2007 international workshop on Domain driven data mining*. 2007, ACM: San Jose, California.
21. Gómez-Pérez, A., M. Fernández-López, and O. Corcho, *Ontological Engineering*, X. Wu and L. Jain, Editors. 2004, Springer-Verlag London Limited: London.
22. Biplab K. Sarker, P.W., Will Gill, *Some Observations on Mind Map and Ontology Building Tools for Knowledge Management.* Ubiquity, 2008.
23. C. Palmer, P.W.Ã., *A computer tool for batch hazard and operability studies.* J. Loss Prev. Process Ind., 2008. **21**: p. 537-542.
24. R. Ferdous, F.K., B. Veitch, P.R. Amyotte, *Methodology for computer aided fuzzy fault tree analysis.* Process Safety and Environmental Protection, 2009. **7** p. 217-226.
25. H.S Pan, W.Y.Y., *Fault Tree Analysis with Fuzzy Gates, .* Computers Ind. Engineering, , 1997. **33**: p. 569-572.
26. F. I. Khan, S.A.A., *Technique Methodologies for Risk Analysis in Chemical Process Industries.* Journal of Loss Prevention in Process Industry, 1998. **11**: p. 261-277.
27. Lin Cui, J.Z., Ruiqi Zhang, *The Integration of HAZOP Expert System and Piping and Instrumentation Diagrams.* Process Safety and Environmental Protection, 2010. **88**(2010): p. 327-334.
28. Chang Chun Chien, Y.C.-C., *Online Fault Diagnosis Using the Signed Directed Graph.* Industrial & Engineering Chemistry Research, 1990. **29**(7): p. 1290-1299.