

Design of Fault Semantic Networks to Integrate Fault, Failure, Hazard, and Accident Models for LNG Plants

Hossam A.Gabbar*, Faisal I.Khan**

*Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology, 2000
Simcoe St. N., Oshawa, L1H 7K4 ON, Canada {hossam.gabbar@uoit.ca}

**Department of Chemical Engineering, College of Engineering, Qatar University, Doha, Qatar 2713

**Process Engineering, Faculty of Engineering & Applied Science, Memorial University, ST John's, NL,
Canada

Abstract

Risks associated with LNG production facilities are related to faults, failures, hazards, and accident scenarios. Understanding and modeling all possible scenarios will support risk prediction, prevention, or mitigation. This paper presents possible modeling approach to integrate faults, failures, hazard, and accident scenarios using fault semantic network or FSN. The proposed approach is applied on LNG production facilities to construct fault propagation scenarios, qualitatively. The proposed approach is used to risks in different design and operation activities.

1. Introduction

LNG is a valuable energy source that is receiving higher attention for cleaner and efficient energy supply. There are risks associated with LNG production processes that require appropriate safety analysis practices. Safety analysis is based on understanding all faults, failures, hazards, and accident scenarios along with the associated risks that might occur in the underlying LNG process. There are different sources to construct and verify these scenarios, such as: (a) understanding process upsets using real time process data; (b) analyze process equipment failures and the associated maintenance work; (c) analyze operational troubleshooting data; (d) analyze fault simulation data; and (e) and analyze engineering design data which includes hazard assessment reports. Risks should be explained and estimated for each scenario from these sources which support decision making related to plant operation and design.

There are different techniques used to reduce risks in LNG plant processes. Such as risk analysis, mitigation, reduction, and management. Process monitoring techniques are developed significantly so that it can provide fault propagation analysis and risk prediction prior to any serious deviations or process upset. This is discussed by many researchers in different disciplines and views. Predictive maintenance is used to estimate remaining life through condition monitoring of equipment failures [1]. Predictive maintenance is mainly based on understanding of equipment good condition and degradation criteria and use to predict remaining life [2]. This technique is useful when one failure is assumed to contribute to the degradation of process equipment [3]. This will be more complex when more than one failure contributes to process degradation or upset. The understanding of equipment degradation with

multiple failures requires developing fault propagation scenarios with the consideration of multiple failures. This paper presents a method to model multiple fault propagation models with degradation and process condition information that are used for accurate fault and accident forecasting. This paper will discuss practical modeling approach for faults, failures, degradations, hazards, and accident scenarios using fault semantic network or FSN which will enable the integration among these scenarios in qualitative and quantitative manner. The proposed modeling approach is applied on LNG production plants to provide risk-informed decisions related to design and operational activities. The first section will provide an introduction about LNG process. This is followed by fault / accident modeling with examples from LNG plants. This is followed by the proposed FSN representation mechanism. Finally, system design and implementation is explained, which is followed by conclusions.

2. LNG Process Description

Liquefied natural gas, or LNG, is natural gas, mainly methane (CH₄). It is temporarily converted into liquid form for ease of storage and transportation. Typically, it is converted into liquid when the production location is far from the usage location. The process starts with treatment in a gas processing units where higher molecular weight hydrocarbons, sulfur compounds and water are removed. This is followed by feeding treated gas into the liquefaction process where it is cooled down. The cooling is typically done using two or three cooling cycles so that the liquefaction temperature reaches -160°C (- 256 °F). The cold liquid LNG is then moved to well-insulated storage tanks at atmospheric pressure. These tanks are loaded into LNG tankers for distribution / shipment. Each of the cooling cycles requires a very large compression train which is usually driven by a gas turbine. In Qatar, the 8 Mtons/y plants are typically based on three trains each is driven by a 125MW Fr9E gas turbine.

There are several LNG accidents that happened in the past. Some of these accidents led to fire and explosion. For example, in October 1944, Cleveland, Ohio, particularly, at the Cleveland peak-shaving plant a tank failed and spilled its contents into the street and storm sewer system. The resulting explosion and fire killed 128 people. The tank was built with a steel alloy that had low-nickel content, which made the alloy brittle when exposed to the extreme cold of LNG. Other LNG accidents led to spills or leak. For example, early 1965, Methane Princess Spill - LNG discharging arms were disconnected prematurely before the lines had been completely drained, causing LNG liquid to pass through a partially opened valve and onto a stainless steel drip pan placed underneath the arms. This caused a star-shaped fracture to appear in the deck plating in spite of the application of seawater. The analysis of these accidents will provide basis to develop accident forecasting techniques [5].

3. Fault / Failure / Hazard / Accident Modeling

Fault is defined as abnormal situation of process or equipment. Faults can be interpreted as symptoms for failures. For example, high pressure is fault in process vessel, which might be

associated with failure like clogged outlet pipes. Hazard is the potential to cause harm to human, facility, or environment. Electric shock or fire could be hazards that might cause harm to human, facility, or environment. Accident is the unpleasant outcome of failure escalation that are associated with losses in human, facility, or environmental stresses. Hazard is the logical factor that if happened might lead to accidents. Figure 1 shows example of corrosion as initial event that might lead to leak. Both are failures. Hazard such as fire might be caused by the leak along with other factors, i.e. the three triangle of the fire: heat, oxygen, and fuel. Fire might be escalated to an accident.

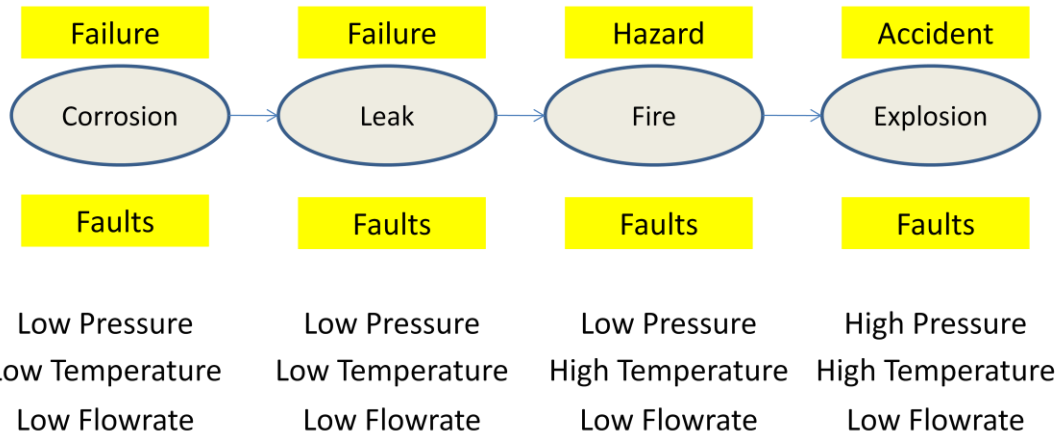


Figure 1. Example of Fault, Failure, Hazard, and Accident Models

The capturing of failures, faults, hazards, and accident are performed in different time frame and by different groups and systems. Table 1 shows possible data capturing of these elements and the corresponding time / groups.

Table 1. Data Capturing Cycle of Fault, Failure, Hazard, and Incident/Accident

	Fault	Failure	Hazard	Accident / Incident
Design	Y	Y	Y	N
Procurement	N	Y	N	N
Installation	Y	Y	Y	Y
Operation	Y	Y	Y	Y
Maintenance	Y	Y	Y	Y

Failure, fault, hazard, and accident causation models are structured and represented using FSN, as explained in the following section.

4. Fault Semantic Network (FSN)

In view of the proposed process model using Plant Process Object Oriented Modeling Methodology (POOM), fault semantic network is utilized to construct flexible fault knowledge structure in qualitative manner, as shown in figure 4. Initially FSN is constructed based on ontology structure of fault models on the basis of POOM where FM or failure mode is described using symptoms, enablers, process variables, causes, and consequences. Rules are

associated with each transition of the causation model within FSN, as shown in figure 2. For example, failures related to leak might be associated with rules such as “IF (Structure.Material = (X or Y)) and (PV= Pressure) and (Dev = Very-High) THEN (FM = Fracture).” These rules are initially defined in generic form based on domain knowledge, i.e. regardless of plant specific knowledge. These rules are further explained for plant specific, i.e. rules associated for tank-1 and pipe-2. Formal language is proposed to represent process domain knowledge and safety control rules, as explained in [4]. Formal language facilitates the synthesis and validation of fault models within FSN. The constructed FSN will be maintained and utilized as part of the proposed fault simulator as explained in the next section.

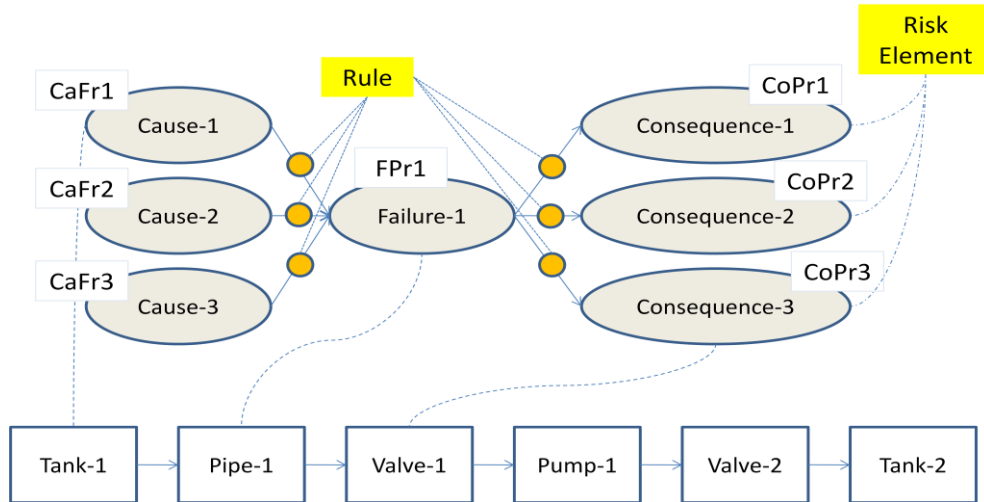


Figure 2. Fault Semantic Network

Risk element is identified for each hazard / fault propagation scenario from the (root) causes to the final consequences. In figure 2, there are three possible risk elements associated with consequence-1: [a] cause-1, failure-1, consequence-1; [b] cause-2, failure-1, consequence-1; and [c] cause-3, failure-1, consequence-1. CaFr1 is used to define the frequency of cause-1. FPr1 is the probability that failure-1 will occur (i.e. due to any cause). CoPr1 is the probability that consequence-1 will occur (i.e. due to any cause & failure). We consider total magnitude of the consequence is Colm1, which is the total impact of consequence-1. For independent events, total risk associated with consequence-1 is shown in equation [Eq1].

$$R(\text{Consequence-1}) = [(CaFr1 + CaFr2 + CaFr3) * FPr1 * CoPr1] * Colm1 \quad [Eq1]$$

Similarly, total risk of consequence-2 and consequence-3 can be computed. In case, events are dependent, then Bayesian theorem should be used to determine the total risk based on dependencies for cause-1, cause-2, and cause-3. as shown in equation [Eq2].

$$P(X|A) = \frac{P(A|X)P(X)}{P(A)} \quad [Eq2]$$

5. System Design & Implementation

The structure of the proposed FSN follows the design explained by Gabbar [4]. The proposed FSN is developed in two layers: static (or offline) and dynamic (or online). Static FSN includes failure / fault / hazards / accidents as structured and linked in the form of causation models,

which are associated with process equipment, as individually and between adjacent process equipments. Dynamic FSN is constructed using dynamic real time or simulated process data from operation, maintenance, safety, and control. In the following section, the system architecture to manage FSN is explained.

5.1 Proposed System Architecture

The proposed system architecture, as shown in figure 3, is selected carefully to capture qualitative / quantitative fault, failure, hazard, and accident data. Real time data is captured from DCS and analyzed using code written in Matlab/Simulink. CAPE-ModE [4] is developed within MS Visio to capture and structure process design models for Process Block Diagrams (PBD), Process Flow Diagram (PFD), and Piping and Instrumentation Diagram (P&ID), based on ISA-S95 / 88. FDS, or fault diagnostic system, is developed to construct fault models using qualitative – quantitative, and deterministic and probabilistic techniques. Fault simulator engine is developed within Matlab / Simulink where fault propagation, equipment reliability, material degradation are calculated and used to construct / maintain fault/failure propagation models. CFD or computational fluid dynamics tool is used to evaluate the granular level of process and equipment condition data such as temperature/pressure profile within a process vessel, or corrosion profile in pipeline body.

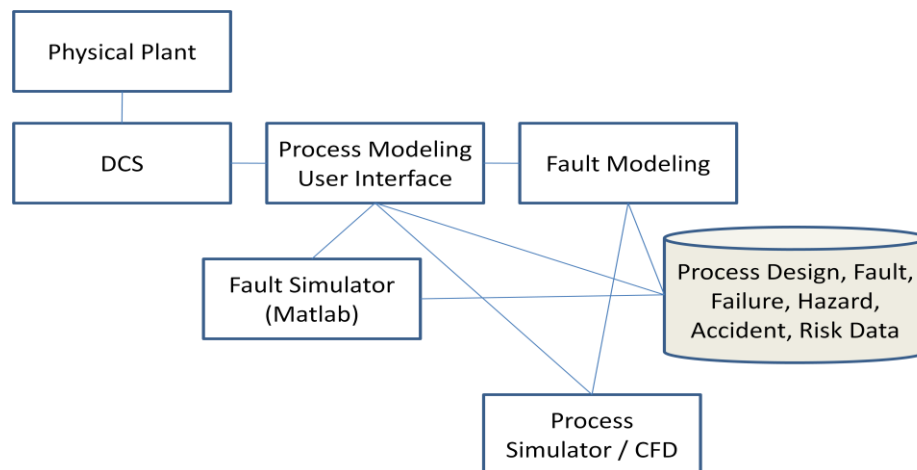


Figure 3. Proposed System Architecture for Failure, Fault, Hazard, and Accident Data Acquisition

5.2 Fault – Failure – Hazard – Accident Knowledge Modeling

The structure of process equipment data group has been designed based on Plant/Process Object-Oriented Modeling Methodology (POOM) where plant structure, behavior, operation, control, and functional views along with the interrelation among them are described in hierarchical manner. Failure and faults are represented in generic level and plant equipment specific level, FM-ID is used to represent both faults and failures. Faults are the combination of process-variable and deviation, e.g. High Pressure. Failures are mechanical, electrical, or material failures. For example, corrosion is a mechanical failure, short-circuited is electrical failure, and material degradation / contamination is a material failure. Human failure / fault could be represented in the same way. For example, human concentration degradation is a fault, while human loses concentration is a failure. Hazard and accidents are modeled in header and

details entities which are linked with lessons learned and controls available / proposed at each step in the causation mode. The controls could be for prevention, mitigation, or detection. Controls could be in the form of actions like engineering, administrative, or operational activities. Figure 4 shows the relationships developed in FSN database, within MS Access.

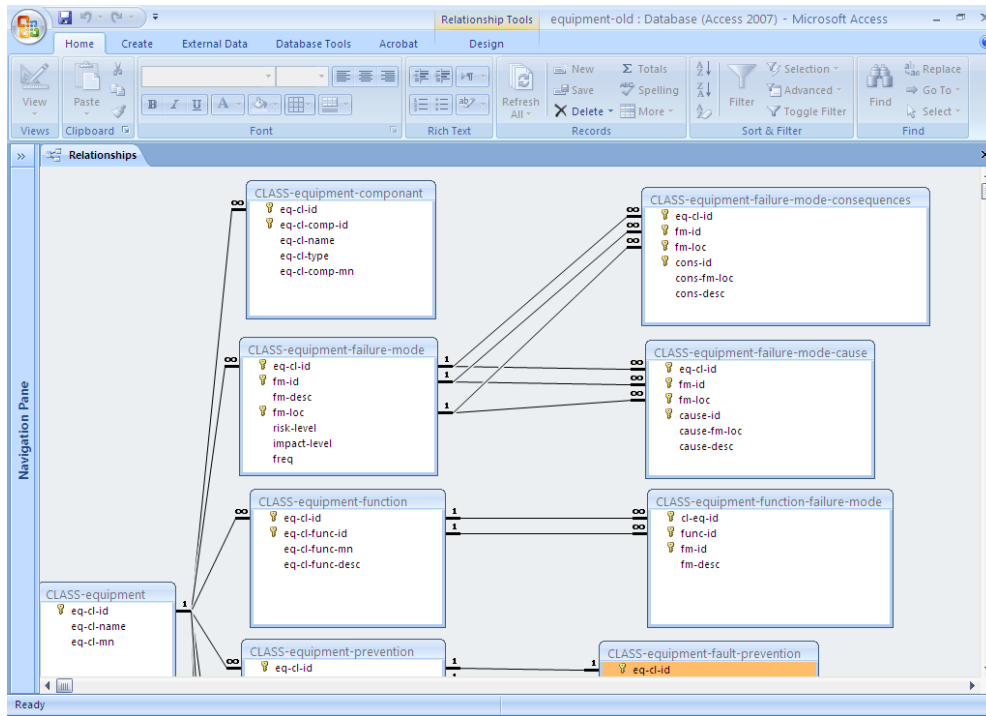


Figure 4. Snapshot of the Relationships in FSN Database

Accident data are collected in excel file which includes two major sheets: header and details.

5.3 LNG Failure / Fault / Hazard / Accident Data Acquisition

The proposed accident analysis focuses on accidents related to LNG (Liquefied Natural Gas), GTL (Gas to Liquid), and NGL (Natural Gas Liquids) processes. At the beginning, engineer will define related set of equipment classes along with their parent class such as “PUMP” and “CENTRIFUGAL PUMP”. Each class is defined as ID and description. Equipment class is related to function, component, and process variables, as shown in figure 5.

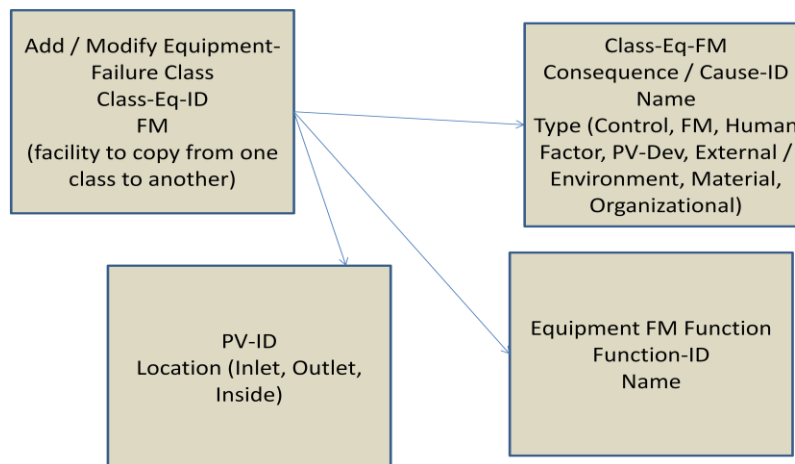


Figure 5. Proposed Data Acquisition Process

6. Conclusion

LNG production facilities are facing challenges to reduce risks. Fault, failure, hazard, and incident/accident are different views that might lead to operational risk in LNG facilities. It is important to provide systematic modeling technique to integrate these views. Fault semantic network or FSN is proposed to integrate these views in generic level and plant specific level. Causation models are developed to link causes, failures, consequences, and controls involved at each escalation step. Fault / failure propagation is linked with hazards and accidents to enable the accurate risk calculation of different accident scenarios while knowing all possible root causes and their propagation and the appropriate controls. FSN is designed to systematically integrate these views and facilitate the data acquisition during process engineering design, operation, maintenance, and other lifecycle activities. Process variables are identified with each fault / failure scenario so that real time and simulated data can be analyzed and linked with hazard / accident scenarios. Failure and accident data are captured from previous LNG accidents and maintenance data to validate the proposed design of FSN.

Acknowledgement

Authors thankfully acknowledge financial support provided by Qatar National Research Foundation through National Priority research project number 08-074-2-015. Thanks for the research students at UOIT who helped in collecting and consolidating LNG accident data. Thanks to collaborators from Japan for providing accident data about LNG processes.

References

- [1] R. C. M. Yam, P. W. Tse, L. Li, P. Tu. Intelligent Predictive Decision Support System for Condition-Based Maintenance [J], the international journal of advanced manufacturing technology, 2001, 17: 383-391.
- [2] K. S. Lu, R. Saeks. Failure prediction for an on-line maintenance system in a Poisson shock environment, IEEE Transactions on Systems, Man, and Cybernetics, 1979, 9(6): 356–362.
- [3] Ghislain Verdier, Nadine Hilgert, Jean-Pierre Vila. Adaptive threshold computation for CUSUM-type procedures in change detection and isolation problems [J], computational statistics and data analysis, 2008, 52: 4161-4174.
- [4] Hossam A.Gabbar, Qualitative Fault Propagation Analysis. Journal of Loss Prevention in the Process Industries, Vol. 20, No. 3 (2007), 260–270.
- [5] <http://www.incidentnews.gov/>

Authors



Dr. Hossam A. Gabbar is Associate Professor in the Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology (UOIT). He obtained his Ph.D. degree (Safety Engineering) from Okayama University (Japan) and worked in process control and safety in research and several industrial projects. Since 2004, he was tenured Associate Professor in the Division of Industrial Innovation Sciences at Okayama University, Japan. Since 2001, he joined Tokyo Institute of Technology and Japan Chemical Innovative Institute (JCII), where he participated in national projects related to control and safety design and operation for green production systems. He developed new methods for automated control recipe synthesis and verification, safety design, and quantitative and qualitative fault simulation. He is a Senior Member, the founder of SMC Chapter - Hiroshima Section, the founder and chair of the technical committee on Intelligent Green Production Systems (IGPS), and Editor-in-chief of International Journal of Process Systems Engineering (IJPSE) and editorial board of the technical committee on System of Systems and Soft Computing (IEEE SMCS). He is invited speaker in several Universities and international events, and PC/ chair / co-chair of several international conferences. He is the author of more than 90 publications, including books, book chapters, patent, and papers in the area of safety and control engineering for green and production energy systems.



Dr. Faisal Khan is a professor and Qatar Gas Chair, in Qatar University. He is also a professor in Process Engineering, Faculty of Engineering & Applied Science, Memorial University, Canada. He obtained his PhD from Pondicherry University, India, 1998. His research interests include process safety and quantitative risk assessment, Risk and reliability engineering, Environmental risk assessment, Risk based decision making.