Activity Modeling for Qualitative and Quantitative Fault Simulation of Nuclear Power Plants

Hossam A.Gabbar
Faculty of Energy Systems & Nuclear Science, University of Ontario Institute of Technology, 2000 Simcoe St. N., Oshawa, ON L1H 7K4, Canada, E-mail: Hossam.gabbar@uoit.ca

Abstract

There is an increasing interest to find an effective mechanism of fault diagnosis for nuclear power plants. Fault simulation has been adopted by many production organizations to evaluate fault propagation scenarios, which is essential for safe plant operation and optimized maintenance. This paper presents an integrated framework for fault simulation where activity models for engineering practices of fault diagnosis are constructed on the basis of IDEF0. The proposed fault simulation framework is based on constructing qualitative fault models in the form of fault semantic networks (FSN) and defining quantitative fault models using statistical and probabilistic techniques. Static and dynamic fault propagation scenarios are synthesized in view of CANDU process models, which are constructed using POOM or plant/process object oriented modeling methodology. The proposed fault simulator framework will improve engineering life cycle activities during the design and operation of nuclear power plants.

Keywords: Fault Diagnosis of Nuclear Power Plants, POOM, Fault Simulation, Fault Diagnosis, Fault Propagation Analysis, Quantitative and Qualitative Fault Models, Fault Semantic Network (FSN).

1. Introduction

Faults are abnormal conditions that might occur in plant equipment, process, or surrounding environment. Faults might be triggered by several reasons such as human error, equipment / part deterioration, equipment failure (which is the complete termination of the function), system error, control device error, environmental stress (e.g. earthquake), or material deficiencies. Fault diagnosis can be viewed as intelligent engine that detect faults, analyze causes and consequences, and estimate the associated risks. Early fault diagnosis will lead to optimized operation and maintenance with reduced risks where it is possible to take suitable counteractions before fault escalates [1]. Although operator support and proactive and predictive maintenance are concerned with fault diagnosis, however, still complete and accurate fault diagnosis is considered as an active area of research. The difficult side of fault diagnosis is to understand current condition, symptoms, and to identify possible (root) causes and final consequences of process upset scenarios. The first step towards fault diagnosis is condition monitoring. There are number of fault diagnosis techniques and tools that are developed by both R&D and industry to provide means to detect and diagnosis process and equipment faults and failure modes. From the other hand, fault simulation is considered as the cornerstone for engineering activities of nuclear power plants. However, fault simulation practices are widely conducted on case-by-case basis where simulation practitioner create fault scenario or

select certain malfunction and identify the affected process variables or structural conditions, and conduct the simulation accordingly. This cannot guarantee completeness of the analysis of all possible fault propagation scenarios. In addition, it doesn't provide practitioner with associated risks and root causes and possible consequences. Simulation is an essential part of engineering activities for the design and operation of nuclear power plants. Figure 1 shows the use of simulation as part of engineering activities of nuclear power plants.

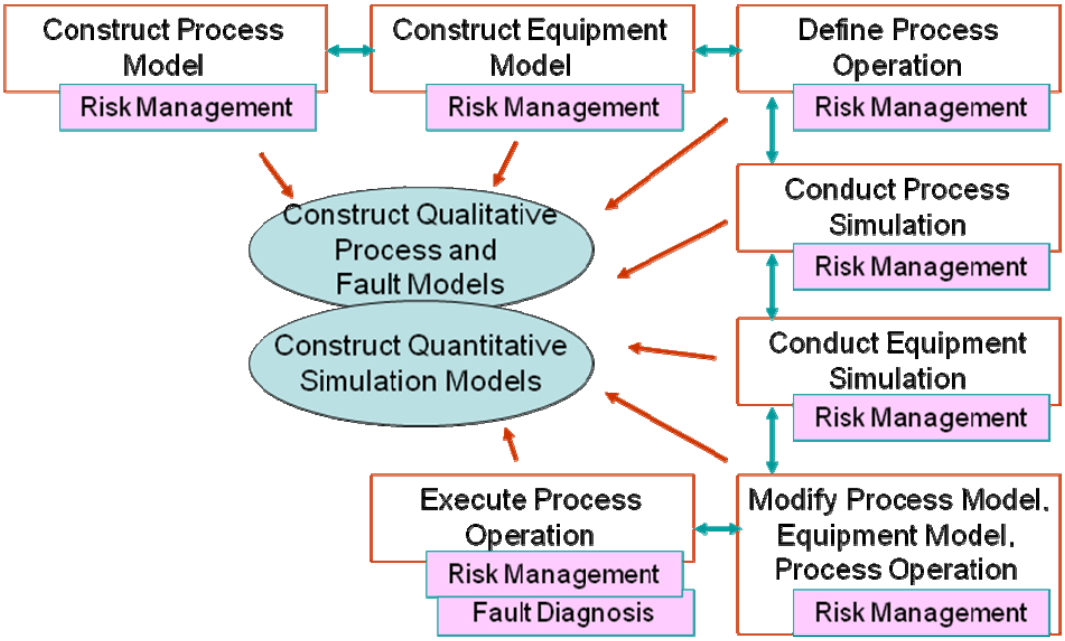

Figure 1. Risk-Based Simulation Practices for Life Cycle Engineering of Nuclear Power Plants

In this research paper, engineering activities for typical nuclear power plants are proposed based on integrated qualitative and quantitative fault modeling and fault analysis methods, as in the following sections.

1.1. Qualitative Methods

There are few qualitative methods that are proposed for fault diagnosis. Fault Tree Analysis or FTA is widely used for fault diagnosis and risk analysis where top events, which are the expected or discovered failure or fault, are linked with consecutive causes in chained manner [2; 3]. It can be associated with risks for quantitative analysis. Failure Mode and Effect Analysis or FMEA, is widely used for fault diagnosis and risk analysis. It shows possible failure modes in plant equipment and parts associated with their consequences. However, FMEA can list only known failure modes. Bond graph is yet another method that has been used for qualitative fault diagnosis [1]. In such method, formal modeling scheme integrating qualitative reasoning with bond graphs is proposed to generate qualitative models to represent system structure and to predict system behavior for diagnosing system failures. Unfortunately, most of the results

obtained from FTA, FMEA, or other qualitative methods are performed using human experience or available knowledge, but not verified quantitatively [4; 5].

1.2. Quantitative Methods

There are several quantitative methods that are reported in the literature as improved quantitative fault diagnosis techniques. Multivariate analysis techniques are used widely for fault diagnosis, such as the use of feature extraction methods for fault detection and diagnosis. Most known methods include: Principal Component Analysis (PCA) [6], Fisher's Discriminant Analysis (FDA), Partial Least Squares (PLS), and Discriminant Partial Least Squares (DPLS) [7; 8]. Features extraction has many applications such as signal classification, fault diagnosis, and many others. PCA has played a prominent role in features extraction and classification problems. Although that, FDA has been shown recently that it gives better results than PCA [9]. Due to the linearity nature of FDA, a lot of classification mistakes occur. Baudat [10] has proposed Kernel version for FDA for two-class problems and multi-class problems. Kernel approach solved the problem of nonlinearity but still choosing the kernel function in order to obtain the optimal nonlinear feature transformation is an open research problem.

1.3. Integrated Qualitative & Quantitative Methods

The idea of utilizing integrated quantitative and qualitative techniques for fault diagnosis is not new. Integrated framework was proposed based on constructing knowledge structure for qualitative and quantitative fault diagnosis information [11; 12; 13]. In such approach, fuzzy logic was used to convert quantitative information into qualitative fault diagnosis knowledge so that fault origin hypothesis can be validated [11]. Vachhani [14] showed another example of integrated quantitative and qualitative approach for fault diagnosis where signed-directed graphs (SDG), as a qualitative technique, is used to generate a hypotheses set of all possible root causes and possible consequences. These generated hypotheses are validated and ranked using nonlinear and statistical estimation, which are validated using simulated examples [14]. Most of other integrated approaches showed construction of qualitative models or graphs which are further tuned and validated using quantitative measures. Such approach is suitable when adequate knowledge is available about how to construct qualitative models. However, in most of the cases there is no enough knowledge about the underlying system, hence qualitative models are not matured and can not be used for effective fault diagnosis. For example, when signed-directed graphs or SDG is used, human experience is mainly used to construct SDG graphs. However, it showed difficulties to construct and maintain graphs during real operation. In addition, it is difficult to reflect the dynamically changing process behaviors and operational aspects into the constructed SDG graphs.

From previous surveys, it is essential to find suitable mechanism to construct and maintain qualitative and quantitative fault models that can be used for fault propagation analysis, which is part of fault diagnosis.

This paper provides integrated qualitative and quantitative fault diagnosis approach where knowledge-based analytical methods [5; 15; 16).are integrated with quantitative methods in such a away that supports the

smooth conversion between qualitative and quantitative models. The proposed approach is based on best practices which are expressed in the form of activity models. The next section shows the proposed integrated fault diagnosis mechanism, which includes explanations of the proposed fault modeling. The integrated qualitative and quantitative fault diagnosis is explained in section 3. Fault diagnosis process and mechanism is explained in section 4. Proposed planning of recovery actions is described in section 5. A selected case study is illustrated in section 6.

2. Integrated Fault Simulation Environment

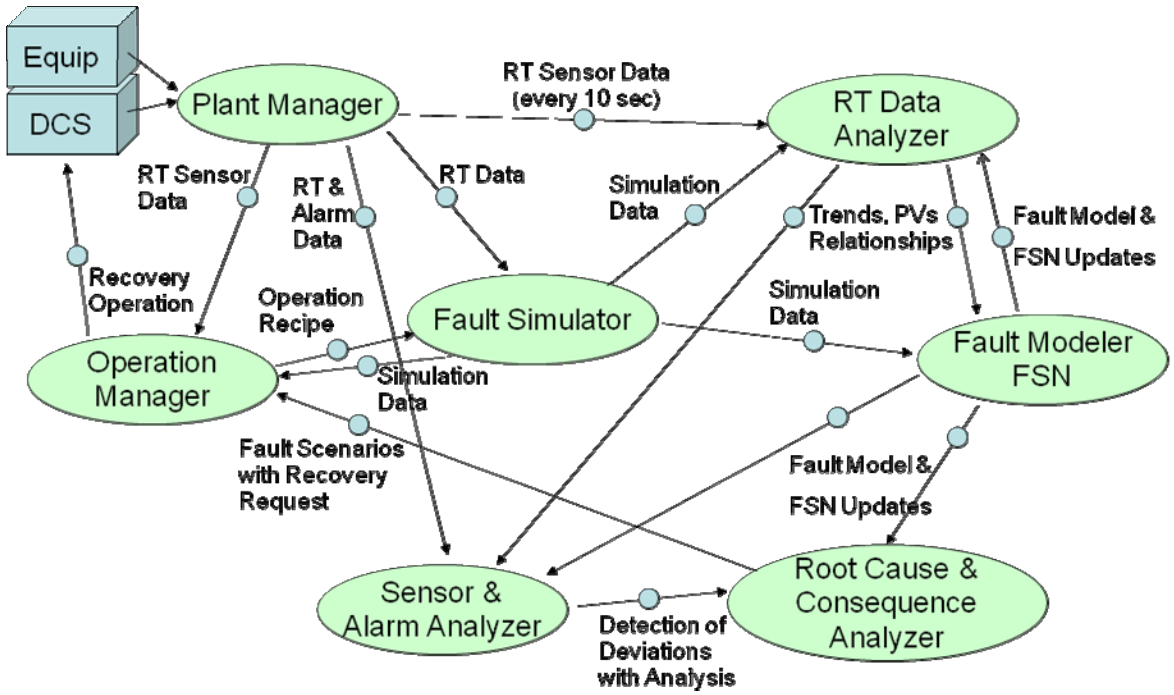

Figure 2. Proposed Integrated Fault Simulation Environment

The proposed integrated fault simulation environment is considered as a decision support to plan and decide design/engineering, maintenance, operation, and management changes/actions in abnormal situations. Figure 2 shows the proposed integrated mechanism where real time data are analyzed and trends are constructed in qualitative manner that can easily be understood by human and process systems and can be integrated within fault models. Similarly, simulation data are analyzed and integrated within fault models, which are used to identify faults and diagnose root causes and possible consequences. Fault models are constructed in the form of fault model libraries that are associated with each structure model element along with their behavior and operation. Fault semantic networks are proposed to structure fault models in terms of process elements, equipment structure, behavior, dynamics, and operation. This is described on the basis of proposed process modeling methodology called POOM, or plant/process object oriented modeling methodology. During the design stage, process simulator is used to extract different trends for normal and abnormal situations, which will be analyzed and converted into quantitative models for effective fault propagation analysis and diagnosis.

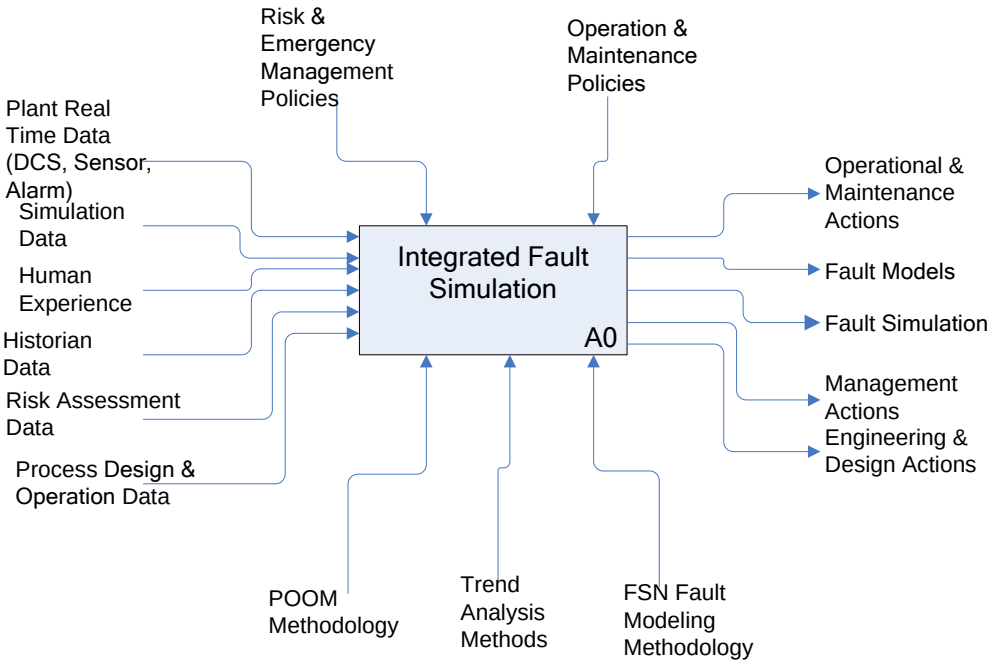

Figure 3. First-Level Activity Model of the Proposed Fault Simulation

In order to understand how to apply and implement the proposed integrated fault diagnosis, detailed activity model of the proposed fault diagnostic system (FDS) is developed using IDEF0 standards [17], as shown in figure 3. The main inputs include process design and operation design data. This includes P&ID, recipe, control instructions, etc. Real time plant data is another input which is extracted from DCS (distributed control system) including sensors (soft and hard sensors) and alarms. Simulation data will be used to predict future behavior and compare with the expected deviations calculated using trend analysis. Human experience will be included to tune fault models and risk ranking. Risk assessment is periodically conducted on production plants. The use of risk assessment results will provide useful fault propagation scenarios with associated risks. The output of the proposed fault diagnosis system is the plan for recovery actions such as maintenance, recovery / shutdown, management change, engineering design change, or system modifications. Corporate risk management policy and operation & maintenance policies are used to control fault diagnosis and decision process. As shown in the above activity model, that the proposed fault diagnosis process utilizes POOM (process object-oriented modeling methodology) and trend analysis method to accurately diagnose all possible faults and deviations in the underlying process, which will be explained in more details in the following sections.

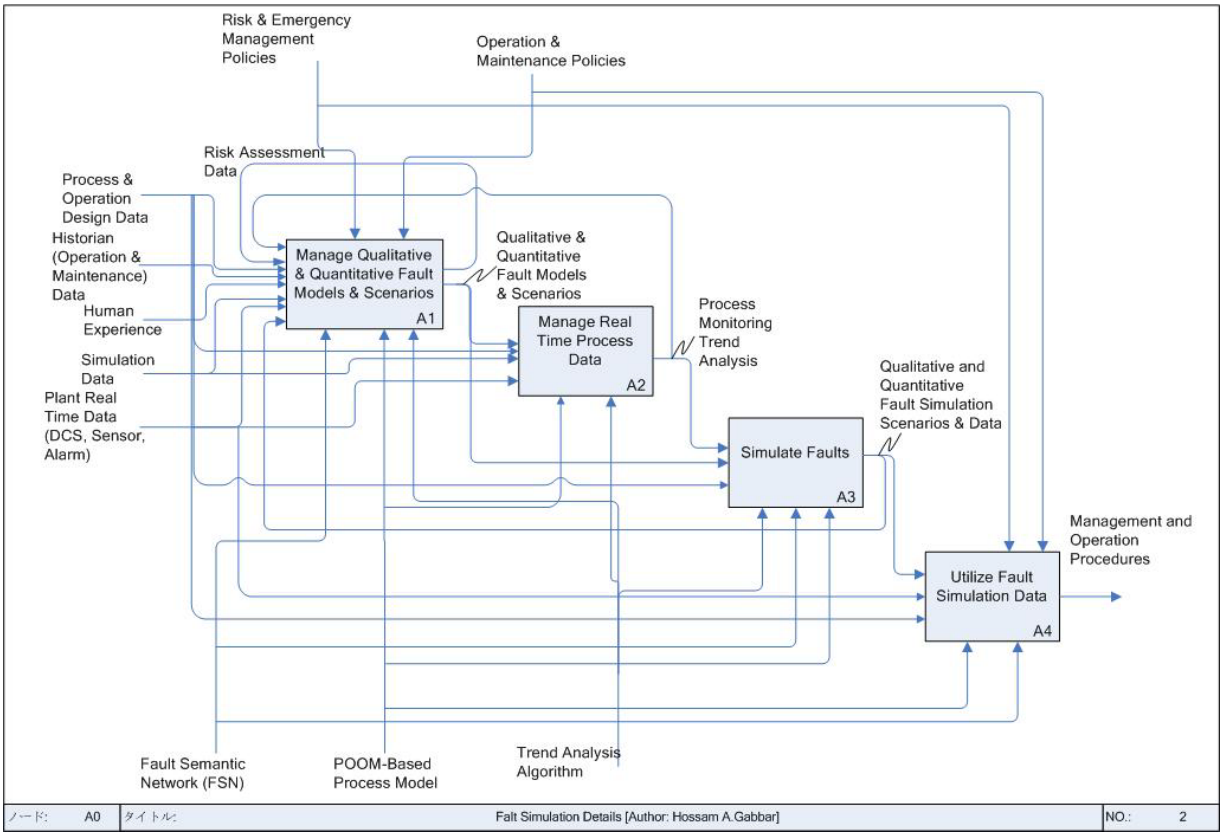

Figure 4. Detailed Activity Model of the Proposed Fault Simulation

The proposed fault diagnosis system is composed of four main processes, as shown in figure 4. The first process is the construction and management of qualitative and quantitative fault models and fault propagation scenarios. The second process is the management of real time process data, including condition monitoring, conversion of raw data into trends, and the analysis of these trends using sensor and trend fusion algorithm. The constructed trends and fault models are used to detect, diagnose faults, and calculate risks for each fault propagation scenario, which is in the third process. The fourth process is concerned with planning and evaluation of recovery actions based on the diagnosed faults.

3. Qualitative & Quantitative Fault Modeling

The proposed fault diagnosis process is based on constructing qualitative and quantitative fault models. Activity model is constructed to show the best practices that can be performed to construct fault models, as shown in figure 5. Fault propagation scenarios are constructed and used to comprehend root causes and consequences and evaluate the associated risks with abnormal situation or process deviation. The proposed qualitative models are further tuned using the developed quantitative models using correlation matrix that provides information about relationships among process variables contributing to each fault. The concept of correlation matrix and its use is described in a separate report and is kept outside the scope of current work. Risk is evaluated using historical data from maintenance history (e.g. reliability data) which are used along with each fault scenario.

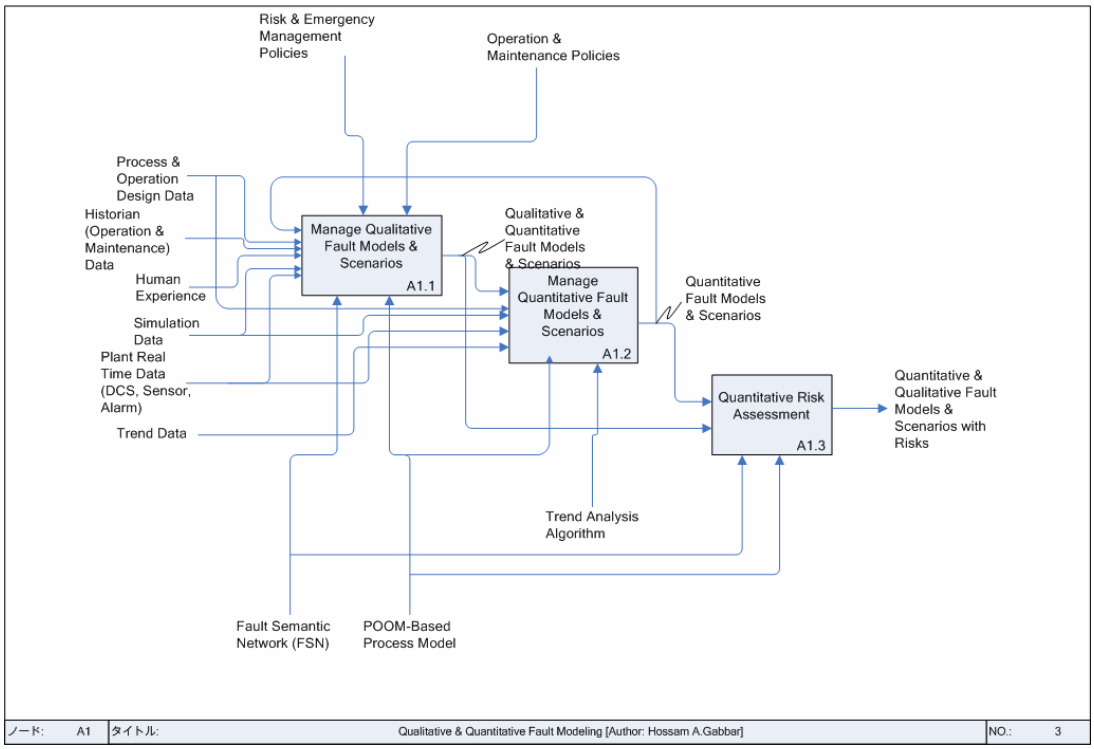

Figure 5. Qualitative and Quantitative Fault Modeling

The proposed fault propagation analysis is conducted by constructing fault propagation scenarios as mapped to plant topology paths [18]. Fault propagation can be described in terms of scenarios that starts from initial event that propagates through process equipments till it reach final consequence. Fault propagation scenarios can be synthesized in online and offline basis. Offline fault propagation can be evaluated using process simulation where different initial events can be identified and fault propagation can be monitored and recorded. These scenarios can be used for real time plant operation. Online fault propagation scenarios can be synthesized from real time plant condition by monitoring fault propagation in plant equipment. Most of current fault assessment practices are based on real time plant operation, where only selected cases are reported and assessed. While, the proposed FPA is based on heuristic approach where all possible fault propagation scenarios are constructed in offline basis, which are used as a repository to select desired fault propagation scenarios in online basis based on real time process condition. The next section describes in details how to synthesize fault propagation scenarios in offline and online basis.

4. Fault Diagnosis Process

It is essential to integrate both computational methods as part of best practices to perform fault diagnosis. The following section describes the detailed activity model that represents best practice of fault diagnosis.

4.1. Fault Diagnosis Activity Model

The proposed fault diagnosis process starts with fault detection using the constructed trends from process condition data [19; 20; 1]. These trends are compared with existing trends with similar operation. If the

trend is found, the corresponding classifier is used to express the fault case. If the trend is not found, new fault case is constructed. Using the proposed fault semantic network (FSN), fault scenario is identified with associated risks, causes, and consequences, as shown in figure 6.

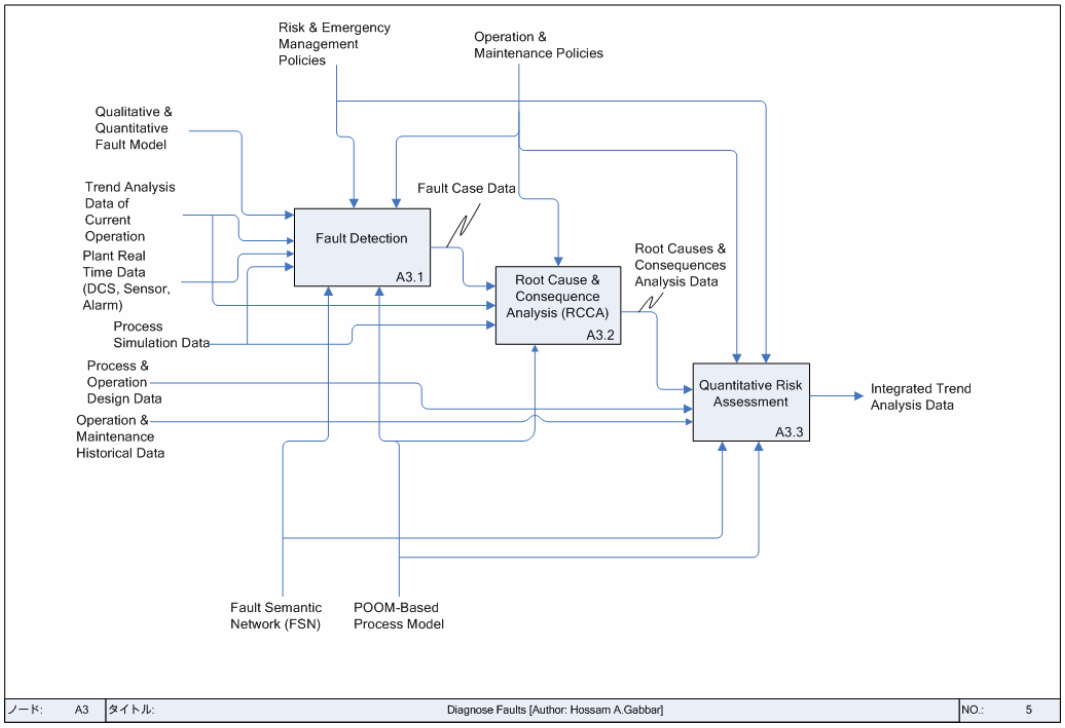

Figure 6. Proposed Fault Simulation Process

4.2. Recovery Actions

Based on the identified faults, recovery actions will be planned, executed, and evaluated. This process is shown in figure 7 where recovery actions could be maintenance tasks, recovery operation, management change, system modifications, or design modifications. The final assessment of recovery action will be used for further tuning fault models for better diagnosis mechanism.

The recovery actions include: shutdown (emergency, partial), startup, and actions related to troubleshooting. In order to design, verify, plan, and execute recovery actions, it is essential to develop detailed activity models as a best practice to manage recovery actions. This will reduce risks associated with recovery actions where actions required by operator and control systems will be clearly defined in proper sequence and estimated values of process variables / conditions.

Detailed activity models are required for different troubleshooting methods such as: Substitution, Circle the Wagons, Fault Insertion, Trapping, and Remove & Conquer. All these methods can be integrated with qualitative and quantitative simulation environment to evaluate each step and provide operator and control system with possible fault scenarios and corresponding consequences, i.e. if no corrective or wrong action is taken.

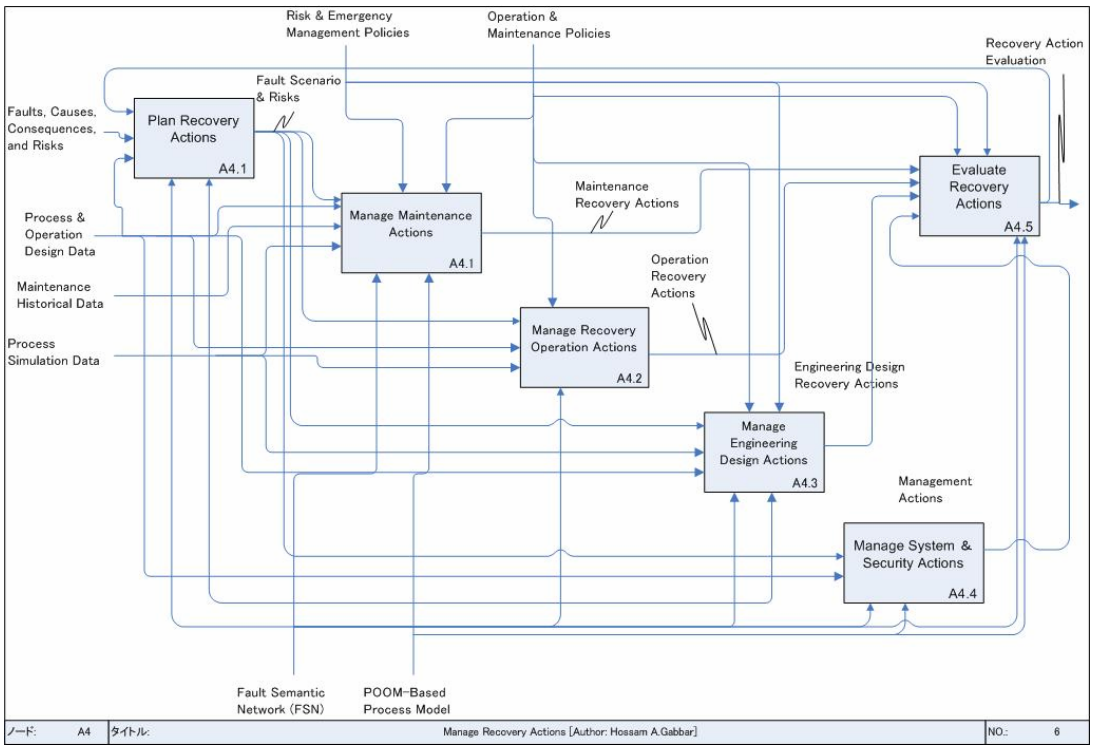

Figure 7. Planning of Recovery Actions

5. Application on CANDU 9

5.1. Malfunction Scenarios

There are number of identified malfunctions that might occur during the operation of CANDU, as expressed in CANDU 9 simulator. For example, PHT LRV fails open which lead to over pressure occurs in heat transport. Traditional quantitative simulation provides information about time taken to reach upper limit, and in case corrective action is considered, how long does it take to return to normal. Qualitative simulation will provide more meaningful relationships between process variables such as valve closure angle and the corresponding pressure or heat level in the steam generator. This will enable operators and engineers to understand all relationships among process variables and failure modes or process deviations, which is essential for decision making for each engineering activity.

5.2. Fault Semantic Network (FSN)

Fault semantic network is a useful technique which allows the representation of domain knowledge related to fault propagation, as shown in figure 8. It shows the basic elements of faults, causes, consequences, symptoms, and related process variables and deviations. It will enable the navigation forward and backwards to understand root causes and possible consequences with the associated risks. It will consider human factors and other environmental stresses that contribute to each malfunction. This will be tuned using real time simulation data using trend analysis techniques which are used to tune rules associated with

each edge within the FSN. In addition, real time data and human experience will be used to further tune associated FSN. PV is used to denote process variables, EV is used for equipment variable (for example open / close angle), FM is failure mode, Eq is process equipment id, and EnV is for environmental variable such as radiation level, pollution, contamination, etc.

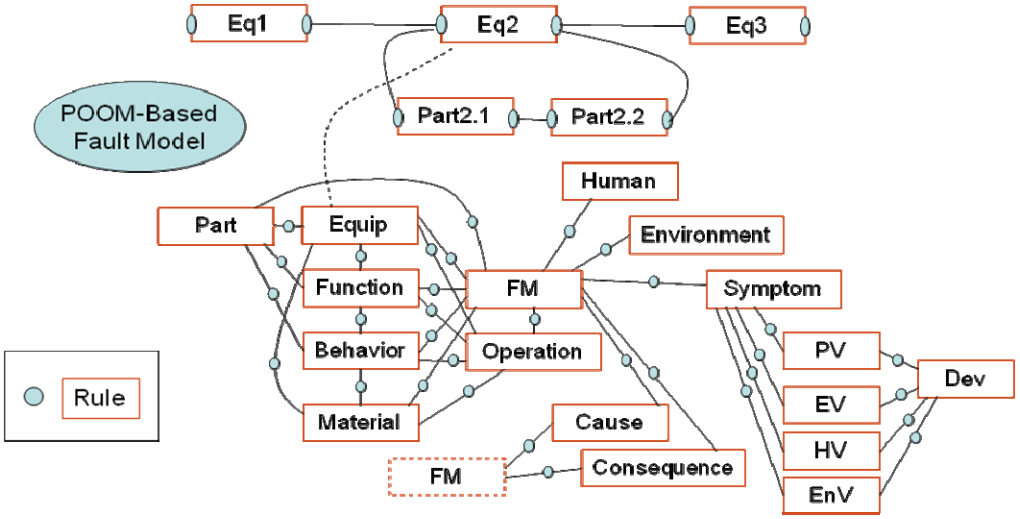

Figure 8. Fault Semantic Network

5.3. Trend Analysis for Quantitative – Qualitative Modeling

The proposed qualitative fault simulation mechanism is based on identifying set of related process variables to each operation so that we can monitor the corresponding trends for these variables. Based on the proposed relationships between controlled and manipulated variables for each operation, trends are obtained using proposed simplified trend fusion algorithm, as shown in table 1.

Table 1. Trend Fusion Algorithm

1. For a given operation, identify control and manipulated process variables
2. Obtain trends for a predefined time window for each process variable, in the form of array of data, e.g. V = [v1,v2, …., vn]
3. Obtain trends for each actionable structure and equipment variables (such as valve, pump, etc.) involved in the underlying operation using the concept of OIA (operation isolation area), e.g. E = [e1, e2, …, en]
4. For the given time window, calculate polynomial regression for all trends and determine polynomial coefficients PC, as a(i,j)
5. Calculate the Z-score for PC which represents $Z(i,j) = [a(i,j) - \mu] / \sigma$
6. Determine the range of Z scores for all normal cases, which are used to differentiate with abnormal cases
7. The resulted trend signature is stored along with the description of each operation and involved materials using symbolic variables to denote the complete operation signature (OS).

For New Cases

Use trend-id, sig-id and compare their signature values with the Z-scores.

If Z-score is within the range, the trend signature is considered for normal operation

OTHERWISE, trend signature is considered for abnormal operation

Each trend is dynamically tuned using new real time or simulation data. Each normal operation is described using normal identifiers in symbolic manner to denote normal operation, while abnormal identifiers are used to denote abnormal or faulty conditions. Trends are obtained for the selected process variables for the time window identified. Actionable structures (e.g. valves and pumps) are represented using uniform distribution (or square signal), for example "1" is used for closed valve, and "0" is used for opened valve. The net trend signature is stored along with each operation details (i.e. symbols for operation description and materials). These values are plotted using MATLAB simulation software to visualize and analyze trends for each operation scenario along with the trend signature and operation signature. The residual value is calculated for each trend using regression equation calculated in MATLAB. This value is the basis of extracting features from trends and therefore concluding the state of operation. Trend signatures are stored within POOM along with their qualitative operation description.

After completing the processing of training data of normal operating conditions and available simulated faults, system can be used to diagnose new cases by selecting the closest operation signature from existing trend data. In case, there is no close trend, the incoming case is marked as new, which will be further analyzed later once available information is obtained. The relationship among process variables, equipment, deviation, and failure modes are identified using the proposed fault semantic network (FSN), which will be dynamically modified using real time operational data and trend analysis results. In addition, human experience will be used to further tune FSN, which are used to identify root causes for any deviation and possible consequences as well as the associated risks.

6. Conclusion

In order to ensure nuclear plant safety, faults and fault propagation scenarios should be adequately understood and analyzed. Although faults are commonly known for CANDU, however, fault modeling is important to identify all possible process upsets and constructing fault models for new designs and technologies of CANDU. There are quite large numbers of mathematical models that can be applied on each fault scenario. The construction of qualitative models can reduce the required number of quantitative models by providing information about the relationships among faults, causes, symptoms, enablers, and consequences. This research work proposes an integrated qualitative and quantitative fault simulation where process design models are constructed on the basis of POOM to facilitate the construction of qualitative and quantitative fault models. Fault semantic network (FSN) is proposed to provide mean for reasoning about root causes and possible consequences as part of fault propagation analysis. Risks are calculated for each scenario using historical maintenance data. Fault models are further tuned using human experience for more meaningful fault diagnosis. Activity models are developed for the proposed fault simulation process to illustrate the engineering practices, activities, and tasks along with their inputs, outputs, controls, and methods in hierarchical manner. Case study CANDU-based nuclear power plant is used to explain few

aspects of the proposed framework of the target fault simulator. In order to map quantitative and qualitative fault models, trends analysis (trend fusion) techniques are proposed where it is used to learn from training data sets, which are used to diagnose new fault cases. Trends are evaluated using simplified trend fusion algorithm, which tune rules and parameters of fault semantic network or FSN. Fault diagnosis and trend analysis results are stored within POOM-based knowledgebase, which is used to support engineering design, operation, and maintenance activities. This will greatly support the move towards next generation nuclear power plants.

REFERENCES

[1] Mano Ram Maurya, Raghunathan Rengaswamy, Venkat Venkatasubramanian, Fault diagnosis using dynamic trend analysis: A review and recent developments, Engineering Applications of Artificial Intelligence Volume 20, Issue 2, March 2007, Pages 133-146.

[2] Haasl, D.F. (1965). “Advanced concepts in fault tree analysis”, System Safety Symposium, Seattle, Boeing Company, 8-9.

[3] Nilsson, A., Årzén, K.E., Petti, T.F.. Model-Based Diagnosis – State Transition Events and Constraint Equations. 1992 IFAC/IFIP/IMACS Int. Symposium on AI in Real-Time Control, Delft, the Netherlands, June 16-18.

[4] Linkens, D.A., Wang, H. (1995), Fault diagnosis based on a qualitative bond graph model, with emphasis on fault localization, IEE Colloquium on Qualitative and Quantitative Modeling Methods for Fault Diagnosis, 24-Apr-1995, pp. 1/1-1/6.

[5] Gabbar, H.A. (2007), Qualitative Fault Propagation Analysis. Journal of Loss Prevention in the Process Industries, Vol. 20, No. 3 (2007), 260–270.

[6] Tutorial on Principle Component Analysis (PCA). http://csnet.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf.

[7] E.K. Kemsley. Discriminant analysis of high-dimensional data: a comparison of principal components analysis and partial least squares data reduction methods. *Chemometrics and Intelligent Laboratory Systems*, 133, 47-61 (1996).

[8] T. Kourti, and J.F. MacGregor. Multivariate SPC methods for process and product monitoring. *Journal of Quality Technology*, 28, 409-428. (1996).

[9] L.H. Chiang, E.L. Russell, and R.D. Braatz. Fault diagnosis in chemical processes using Fisher discriminant analysis, discriminant partial least squares, and principal component analysis, *Chemometrics and Intelligent Laboratory Systems*, 50, 243–252. (2000).

[10] G. Baudat, and F. Anouar. Generalized discriminant analysis using a kernel approach. *Neural Computation*, 12, 2385–2404. (2000).

[11] Yu, C.C., and Lee, C. (1991), Fault Diagnosis Based on QuaIitative/Quantitative Process Knowledge, AlChE Journal, April 1991, Vo1. 37, No. 4., pp. 617-628.

[12] Benkhedda, H. and Patton, R.J. (1996), Fault diagnosis using quantitative and qualitative knowledge integration, UKACC International Conference on Control. Control '96, p. 849 -854.

[13] Castro, A.R. and Miranda, V. (2005). An interpretation of neural networks as inference engines with application to transformer failure diagnosis. International Journal of Electrical Power & Energy Systems, Vol. 27, Issues 9-10, November-December 2005, Pages 620-626.

[14] Vachhani, P., Narasimhan, S. (2007), Rengaswamy R. An Integrated Qualitative—Quantitative Hypothesis Driven Approach for Comprehensive Fault Diagnosis, Chemical Engineering Research and Design, Vol. 85, Issue: A9, pp 1281-1294.

[15] Liu, H. and Coghill, G.M. (2005). A model-based approach to robot fault diagnosis. Knowledge-Based Systems, Vol. 18, Issues 4-5, August 2005, Pages 225-233

[16] Maurya, M.R., Rengaswamy, R., and Venkatasubramanian, V. (2006). A signed directed graph-based systematic framework for steady-state malfunction diagnosis inside control loops. Chemical Engineering Science, Vol. 61, 1790-1810.

[17] IDEF0. http://www.idef.com/Home.htm.

[18] Gabbar, H.A. (2007), Intelligent Topology Analyzer for Improved Plant Operation, Journal of Industrial Management and Data Systems (IMDS), Vol. 107, Issue 2, pp. 229-250.

[19] Gabbar, H.A. (2007), Trend Analysis Technique Using Real Time Fault Simulation for Real Time Fault Diagnosis, IEEE SMC International Conference, Oct-2007, Montreal, Canada.

[20] Sourabh Dash, Mano Ram Mauryaa, Venkat Venkatasubramanian, Raghunathan Rengaswamy, A Novel Interval-Halving Framework For Automated Identification of Process Trends, American Institute of Chemical Engineers (AIChE) Journal, January 2004, Vol. 50, No. 1, pp. 149-162.

Appendix (1) – Abbreviations

DCS: Distributed control system. It is a control system that is widely used within production plants.

DPCA: Dynamic principle component analysis. Is data analysis method obtained by simple modification to PCA.

EQ: Equipment. It is used to denote plant equipment.

ETA: Event tree analysis. It is qualitative and quantitative method to analyze faults

FDS: Fault diagnostic system. An integrated system for fault diagnosis.

FM: Failure mode. It is used to denote failure modes of a given process or equipment.

FMEA: Failure mode and effect analysis. It is a qualitative and quantitative method used to measure system reliability and analyze faults.

FTA: Fault tree analysis. It is a qualitative and quantitative method for fault analysis.

FSN: Fault semantic network. It is proposed by Hossam A.Gabbar to describe knowledge structure of faults / failure modes with their causes and consequences.

IDEF: Integrated Definition Methods used for system and process modeling developed by knowledge based systems KBS Inc. (KBSI).

OPC: OLE for Process Control. It is de facto standards for interconnectivity of process control data.

PCA: Principle component analysis. Is a method for data analysis used to reduce data dimensionality and remove noise by identifying principle components.

P&ID: Piping and instrumentation diagram. It is used to describe process design.

POOM: Plant/process object oriented modeling methodology. This methodology was invented by Hossam A.Gabbar and applied on continuous and batch plants as well as discrete manufacturing processes.

RCCA: Root cause and consequence analyzer. It is a module within FDS proposed by Hossam A.Gabbar to identify all possible causes and reason about all possible consequences.

RT: Real time. It is used with data to denote real time data.

SDG: signed-directed graph. It is a graphical method to represent and model faults along with their causes and consequences.

SU: Structure unit. It is used to denote structure units while constructing process models using POOM.