INL/CON-17-41437
PREPRINT

FAULT PROPAGATION AND EFFECTS ANALYSIS FOR DESIGNING AN ONLINE MONITORING SYSTEM FOR THE SECONDARY LOOP OF A NUCLEAR POWER PLANT PART OF A HYBRID ENERGY SYSTEM

10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC-HMIT)

Huijuan Li, Xiaoxu Diao, Xiang Li, Boyuan Li, Carol Smidts, Shannon Bragg-Sitton

March 2017

FAULT PROPAGATION AND EFFECTS ANALYSIS FOR DESIGNING AN ONLINE MONITORING SYSTEM FOR THE SECONDARY LOOP OF A NUCLEAR POWER PLANT PART OF A HYBRID ENERGY SYSTEM

Huijuan Li[a], Xiaoxu Diao[a], Xiang Li[a], Boyuan Li[a], Carol Smidts[a] and Shannon Bragg-Sitton[b]

[a]Department of Mechanical and Aerospace Engineering
The Ohio State University
201 W. 19th Ave, Columbus, OH 43210
li.6131@osu.edu; diao.38@osu.edu; li.984@osu.edu; li.4935@osu.edu; smidts.1@osu.edu

[b]Idaho National Laboratory
PO Box 1625 MS 3860
Idaho Falls, ID 83415-3860
shannon.bragg-sitton@inl.gov

ABSTRACT

This paper studies the propagation and effects of faults of critical components that pertain to the secondary loop of a nuclear power plant found in Nuclear Hybrid Energy Systems (NHES). This information is used to design an on-line monitoring (OLM) system which is capable of detecting and forecasting faults that are likely to occur during NHES operation. In this research, the causes, features, and effects of possible faults are investigated by simulating the propagation of faults in the secondary loop. The simulation is accomplished by using the Integrated System Failure Analysis (ISFA). ISFA is used for analyzing hardware and software faults during the conceptual design phase. In this paper, the models of system components required by ISFA are initially constructed. Then, the fault propagation analysis is implemented, which is conducted under the bounds set by acceptance criteria derived from the design of an OLM system. The result of the fault simulation is utilized to build a database for fault detection and diagnosis, provide preventive measures, and propose an optimization plan for the OLM system.

Key Words: Fault Propagation and Effects Analysis, Online Monitoring System, Nuclear Hybrid Energy Systems, Secondary Loop

1 INTRODUCTION

Nuclear Hybrid Energy Systems (NHES) are highly complex integrated hybrid energy systems which aim to provide reliable power generation and increase renewable energy penetration into the power grid, and allow for the repurposing of excess electricity in times of low demand. The system dynamics that characterize NHES involve frequent switching between different energy and control subsystems. Frequent switching between different subsystems may lead to faster aging of the mechanical components and sensors, thus leading to shutdown of an energy subsystem. Failure of the energy subsystems will add an unexpected load to the nuclear power plant, therefore increasing the risk of an accident. Nuclear power plants within NHESs are expected to be challenged in a manner which differs significantly from their conventional usage. In particular, it is expected that the secondary loop of the plant will need to adjust to highly fluctuating energy supplied by the renewables. Risk and reliability aspects of the secondary loop of a nuclear power plant within a NHES are tested in such configurations and should be studied systematically. An advanced on-line monitoring system (OLM) can minimize potential component failure, control failure, and human error. Developing such OLM is a complex problem since NHESs in their conceptual design phase are such

that configurations and components are still being identified. Analysis and determination of failure modes of potential components is the first step of designing an on-line monitoring system for the secondary loop. The nuclear power plant follows a typical Pressurized Water Reactor (PWR) design. The secondary loop is a power conversion circuit which uses the Rankine cycle. This loop consists of the main steam lines, turbine/generator, steam dump, condensate/feed system, turbine by-pass systems, main steam safety valves, and steam feed/isolation systems.

In general, the OLM system is independent of the facilities pertaining to the secondary loop located in nuclear power plants. In order to detect faults effectively and precisely, various sensors or probes will be applied to the secondary loop system. Several significant issues shall be studied for sensor application, such as (i) how many sensors should be deployed into the secondary loop system; (ii) what information should be gathered to effectively detect faults; (iii) how to identify the most efficient locations for the layout of sensors considering the trade-off of cost and efficiency. Many studies [1]–[5] studied these problems in other specific industrial fields. In this paper, these issues can be solved by gathering and analyzing potential faults of critical components that constitute the secondary loop system. It is impractical to deploy sensors to observe all the system components and outputs. By investigating the causes, propagation paths, and impact of faults, the design of the OLM system can detect as many critical faults as possible while spending the minimum cost for sensor deployment. A critical fault is a fault that potentially leads to catastrophic or large-scale functional failures. In this paper, the potential faults of basic components, such as the steam generator, steam turbine, etc. are investigated and analyzed via the Integrated System Failure Analysis (ISFA) method [6], which is a promising method for the simulation of fault propagation. Through the ISFA method, the cause and effect of faults that are derived from components of the secondary loop can be collected.

The remainder of the paper is divided into the following sections: Section 2 defines the OLM design methodology associated with fault propagation analysis; Section 3 introduces the application of the ISFA method for analyzing faults of critical components in the second loop system; Section 4 concludes the study and introduces future research.

2 METHODOLOGY OF OLM DESIGN BASED ON FAULT ANALYSIS

Designing an OLM system for the secondary loop system includes several important steps, such as determining the information required for fault detection, deciding how to deploy the sensors, constructing a database for online fault diagnosis, and so on. Many of these steps depend on the detailed information related to potential faults, such as location (e.g. hardware or software components), triggering conditions (e.g. input signals), the propagation path (possibly from hardware to software), fault effects (functional failures), and specific features (i.e. period). This information can be acquired via a fault analysis applied to the secondary loop. The OLM design methodology associated with the fault analysis is defined in Figure 1.

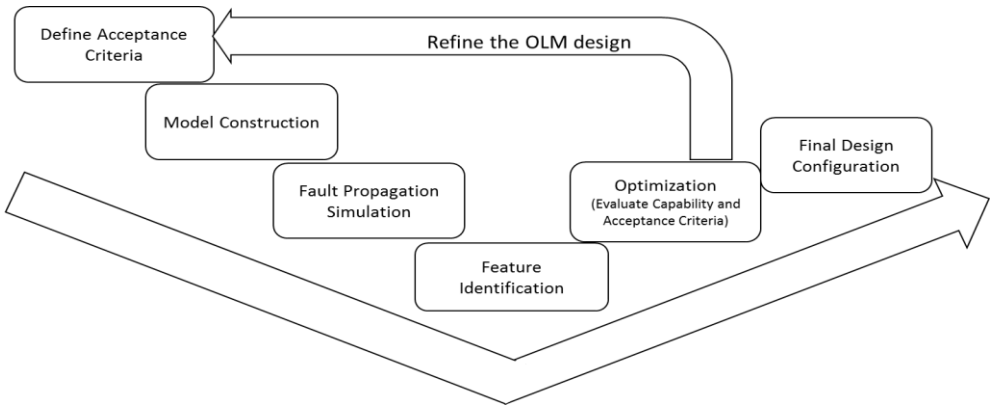

Figure 1 OLM design methodology associated with fault analysis

As depicted in Figure 1, the iterative process for designing an OLM system can be divided into the following processes. The first step is to define acceptance criteria for the proposed OLM design. The second step is to construct the ISFA models of the system under study. The third step is to simulate fault propagation paths. The fourth step is to extract features that will allow us to distinguish the faults. The fifth step is to test the detection and diagnosis capability of the OLM design. If the acceptance criteria are met, the final result is an OLM design configuration that includes a database of behaviors of the system when it is subjected to various faults, a maintenance plan, and a design of additional sensor type and placement. These steps will be defined in the following subsections.

2.1 Acceptance Criteria

Acceptance criteria are used to evaluate the fault detection capability of the OLM system. The satisfaction of acceptance criteria means that the OLM system is able to detect an adequate type and number of faults so that the iterative design and optimization process can stop. Generally, adding sensors is the primary method to enhance the capability of fault detection of the OLM system. A criterion for accepting an OLM design can be defined as:

$$\frac{\Delta R}{\Delta C} < \alpha \tag{1}$$

In Equation (1), the parameter ΔR is the sum of the risk grade of all unidentified faults, and ΔC is the cost of deploying additional sensors. The parameter α is a threshold that can be defined for the specified system. The equation indicates that the design of OLM is acceptable when the cost of adding extra sensors out balances the residual risk of unidentifiable faults.

Another criterion is defined as a stopping condition for fault propagation simulation. In the iteration of OLM design, fault simulation is required to study the behaviors of the secondary loop system when some components are faulty. Therefore, faults will be injected into the model of the secondary loop system during simulation. The stopping condition acts as the indication of whether the number of injected faults is sufficient, so that it is unnecessary to inject additional faults during an execution of the simulation. The evaluation is based on the number of injected faults, defined as:

$$\frac{N_n}{\Sigma_{i=1}^{n} N_i} < \beta \tag{2}$$

In Equation (2), i is the number of faults injected together (staged or simultaneous injection) in an iteration of the OLM design, N_i is the number of new behaviors that occur due to i faults. The system behavior can be observed by sampling the output signals of system components. The parameter β is a threshold that can be defined for the specified system. In practice, the thresholds α and β are usually obtained from experts. Other acceptance criteria can be defined as well.

2.2 Model Construction

The proposed OLM design should be able to detect, identify, and diagnose the propagation of failures for all postulated faults (within the acceptance criteria). In this research, the Integrated System Failure Analysis (ISFA) [6] is used to analyze the propagation of faults. ISFA is an integrated approach that performs the failure analysis of a HW/SW system during the design stages of that system. ISFA integrates the functional failure identification and propagation (FFIP) method [7] for fault propagation and effects analysis of the HW subsystems as well as the failure propagation and simulation approach (FPSA) method [8] for the analysis of fault propagation in the SW subsystems.

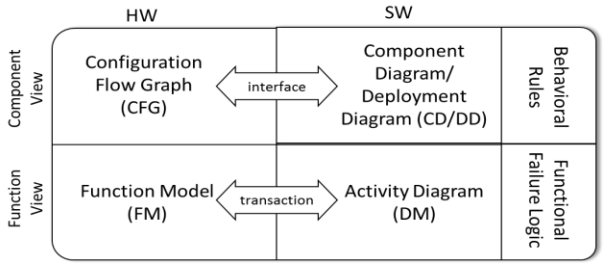

Figure 2 ISFA Method – System Models

As shown in Figure 2, ISFA analyzes the hardware and software subsystems based on a component view and a function view. A configuration flow graph (CFG) is constructed to depict the component structure of the physical system. A functional basis (e.g. a repository of functions) is used as a standard to define functions and flows of all physical components. By connecting predefined functions and flows based on mathematical models, a function model can be constructed to depict how to achieve the desired functionality of the system. Qualitative behavioral models are defined for each component, and are depicted as behavioral rules (BRs) including discrete nominal and faulty behaviors that are derived using qualitative physics. A Function failure logic (FFL) is defined for each component to relate the component behavior and the operating state of system functions. In the component view, HW is integrated with SW via interfaces, which are components that communicate send/receive information between HW and SW subsystems. A transaction signal is defined to depict the communication details of the HW-SW interaction. Based on the ISFA method, the process of analysis is depicted in Figure 3.

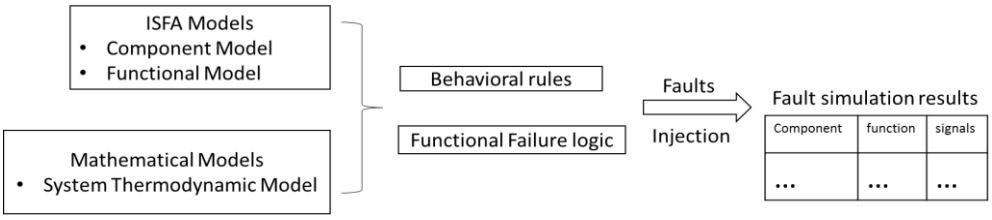

Figure 3 Fault Propagation Analysis Based on ISFA – Steps

As illustrated in Figure 3, two types of models are required by the ISFA method. The ISFA models that include component and functional models are defined to express the structure and function of the secondary loop system. Meanwhile, the mathematical models are investigated in order to formulate the behaviors (including inputs and outputs) of system components in normal and faulty states. Further, their behaviors are expressed by the BRs, and the states of their functions (e.g. operational, degraded, or lost) are assessed by the FFL defined for each component. The fault propagation paths are attained through the ISFA simulation process with fault injection.

2.3 Fault Propagation Simulation

The simulation is performed based on ISFA. Prior to the simulation, the parameters of ISFA models need to be initialized. The attributes of inputs and outputs to the components, such as name, type, range, and other key parameters are defined. The BRs for each system component and the FFLs for possible states of functions are determined. The simulation then executes iteratively for different numbers of faults injected. One fault is first injected and the ISFA simulation is executed to produce new behaviors. Then, multiple faults are injected together. The iterative process will end when the fault injection stopping criteria are met. Finally, we can obtain the ISFA simulation results of all possible fault propagation paths. The number of faults injected N is determined by the stopping criteria defined in equations (1) and (2). To determine the

fault injection time, the behaviors of the system after a fault injection are investigated and evaluated. The system behavior can be observed through the outputs and states of system components. The new behaviors can be defined as the new types or patterns of output signals or state transitions that have not occurred before. In practice, injecting two faults together in an iteration of the OLM design at different time points can lead to new behaviors.

In the secondary loop system, discrete time series of input/output of system components sometimes display a periodicity and fit the model $x = a + s_t + v_t$, where a - trend, s_t - seasonality, and v_t - random noise. Consequently, we use the behavior of one period to represent the behavior of the whole series.

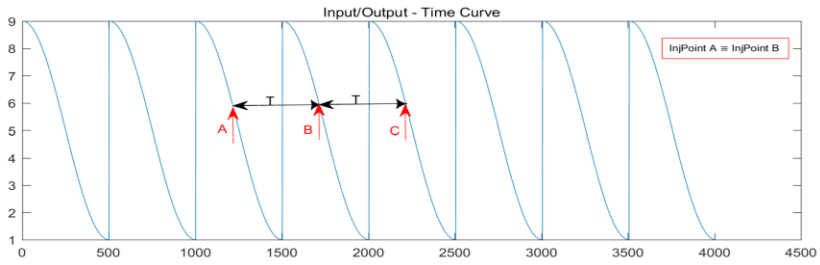

Figure 4 Fault Injection Period

As demonstrated in Figure 4, the consequence of a fault injection will be identical when a fault is injected at time point A and B. Therefore, suppose that Fault 1 is injected at t_1 and Fault 2 after t_1. The possible time of injection of Fault 2 can be restricted to one period of the time series created by injecting Fault 1.

2.4 Identify Features

The outcomes of fault propagation simulation are a series of tables that contain the behaviors (input/output signals) of all components before and after fault injection, and the states of the functions of each component and of the integrated system. This information is later utilized to diagnose the occurrence, location, and type of fault that may have occurred. In the design of the OLM system, these data are classified into observable signals and unobservable signals. An observable signal is a signal that can be detected by the sensors in an OLM design. Conversely, an unobservable signal is a signal that cannot be acquired by the OLM system as designed. For an OLM system, only the observable signals can be used to extract fault features (i.e. the type or pattern of the input/output signals) in order to identify faults. The fault feature vector is composed of the following elements.

- Period T – observable signals display periodicity;
- Mean value reflect the global property of observable signals;
- Principal frequency and its power spectrum density – reflect the frequency characteristics;
- Shannon entropy reflect the states of observable signals by evaluating the amount of randomness;

For the case that fault feature vectors contain high-dimensional data with large amounts of information, Principal Component Analysis (PCA) [9] can be applied to reduce the data dimensionality.

Feature-based fault identification is accomplished through the comparison of fault pairs, which evaluate two faults by contrasting all observable fault-related signals derived from the fault simulation. In the comparison, the degree of contribution is a value $I_j(OS_i)$ defined to estimate whether the observable signal OS_i can help discriminate between two distinct faults pertaining to a fault pair j. The range of the value is $\{0,1\}$, where 0 means that the feature vector values of the observable signal i are identical if one

injects either of the two faults. In contrast, the value 1 denotes that the feature vector values of the observable signal i are totally different. If $\sum_{i=1}^{M} I_j(OS_i) = 0$, where M is the number of observable signals, the two faults in the fault pair j are unidentifiable. Then, the unidentified faults ratio can be calculated as:

$$R_{UF} = \frac{N_{UF}}{PN} \tag{3}$$

In Equation (3), the variable N_{UF} is the number of fault pairs being compared that cannot be distinguished. The parameter PN is the total number of fault pairs to be compared.

2.5 Design Optimization

To improve the detection and diagnosis capability of the OLM system, the features of unidentified faults should be analyzed. This analysis requires the extraction of fault features from unobservable signals. Then, the comparison of unidentified fault pairs is performed to determine which unobservable signals can most improve observability and diagnosticity. The optimization steps are displayed in Figure 5.

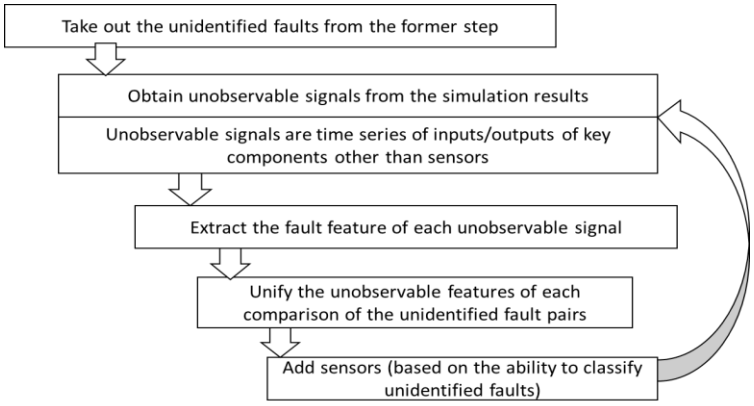

Figure 5 Workflow of the Optimization of the OLM Design

The primary goal of optimization is to increase the number of identifiable faults with minimum costs. This can be achieved by adding sensors into the secondary loop in order to acquire more signals that are currently unobservable. The sensor capable of resolving the largest number of undistinguishable faults is added first to the OLM design. The unobservable signals UOS_i can be evaluated via the degree of contribution to observability (DCO), which is defined as

$$DCO(UOS_i) = \frac{\sum_{j=1}^{PN} I_j(UOS_i)}{PN} \tag{4}$$

In Equation (4), PN is the number of fault pairs. The DCO denotes the ability of the observable signal i to identify faults. The UOS_i then can be ordered according to the DCOs which estimate the ability of signals to identify faults. After adding new sensors into the OLM system, the design and optimization process will be performed iteratively. The iterative process can be stopped when the acceptance criteria in equations (1) and (2) are satisfied.

3 FAULT PROPAGATION ANALYSIS

In this section, we perform the fault propagation analysis for basic components in the secondary loop of a nuclear power plant embedded in a NHES. First, we construct the component and functional models for ISFA. Then, we refer to the mathematic models of these components to create the behavioral rules and

functional failure logics required by ISFA for fault simulation. Finally, we display the results derived from the simulation.

3.1 Component and Functional Models

A secondary loop of nuclear power plant is comprised of several crucial HW and SW components. The HW components encompass a steam generator, turbine, condenser, pump, and various pipes and sensors. The steam generator transfers heat from the primary loop to the water of the secondary loop; the steam turbine extracts thermal energy from pressurized steam and uses thermal energy to produce electricity; the sensors are used to measure system dynamics such as pressure, temperature, flowrate, etc. Important SW components include a configuration manager used to initialize software components, the virtual sensors for reading and calculating system inputs, and the control algorithm for performing valve control. Other components while important are not discussed in this analysis.

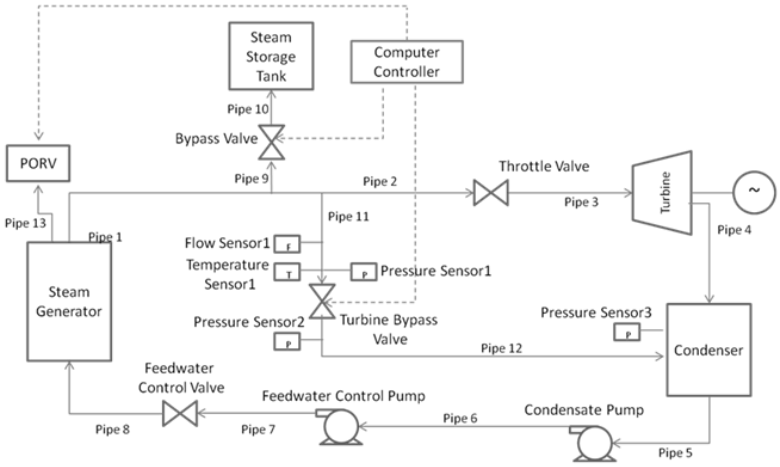

Figure 6 System representation of the secondary loop

Figure 6 provides the system representation. Only the necessary sensors are shown. Flow Sensor1 measures the inlet flow rate of the Turbine Bypass Valve. Temperature Sensor1 and Pressure Sensor1 measure the inlet temperature and pressure of the Turbine Bypass Valve, respectively. Pressure Sensor2 measures the outlet pressure of the Turbine Bypass Valve. Pressure Sensor3 is used to detect if the Condenser is available for dumping steam.

The corresponding component model for ISFA is displayed in Figure 7, in which hardware and software components are described separately. The interoperations between hardware and software components are represented by the concept of interface. In the figure, three interfaces are declared to connect the valve control program to the actual valves in the physical world.

3.2 Mathematical Models

Mathematical models of the secondary loop provide a mechanism to calculate instantaneous values of the parameters pertaining to HW/SW components during ISFA simulation. The secondary loop of the nuclear power plant follows a thermodynamic model, a standard Rankine cycle. A Rankine cycle [10] is a model used to predict the performance of steam turbine systems. This is an idealized thermodynamic cycle (a closed loop) of a heat engine that converts heat into electricity. Figure 8 shows the Rankine cycle used in this analysis. The process in the figure is explained as follows:

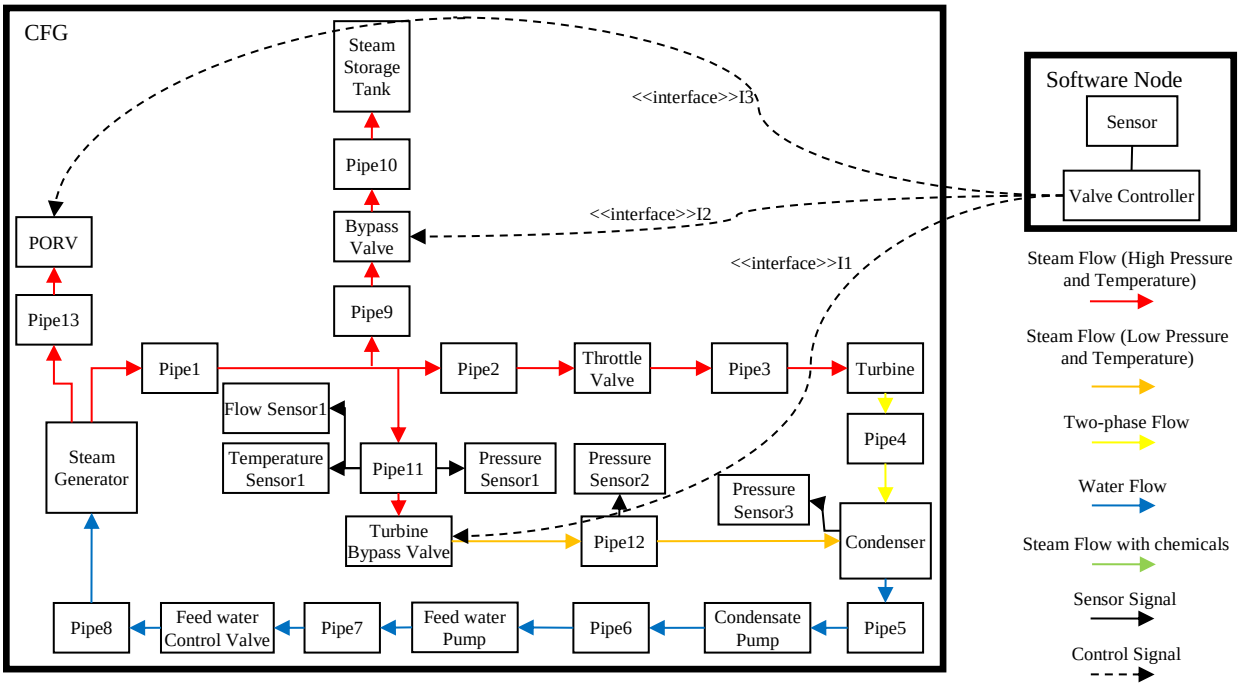

Figure 7 Component Model of the Secondary Loop System

- Condensate pump 1 to 2: Reversible Adiabatic Process, Pressure Increase; The material changes from saturated water at 1 to subcooled water at 2;
- Steam generator 2 to 5: Two-phase Flow Region, Equal Pressure; The material at 3 is saturated water; from 3 to 4 the material is two-phase flow; the material at 4 is saturated steam; the material at 5 is superheated steam;
- Turbine 5 to 6: Reversible Adiabatic Expansion, i.e., Isentropic Process. The material changes from superheated steam to two-phase flow at 6;
- Condenser 6 to 1: Reversible Adiabatic, Equal Pressure. The material changes from two-phase flow to saturated water.

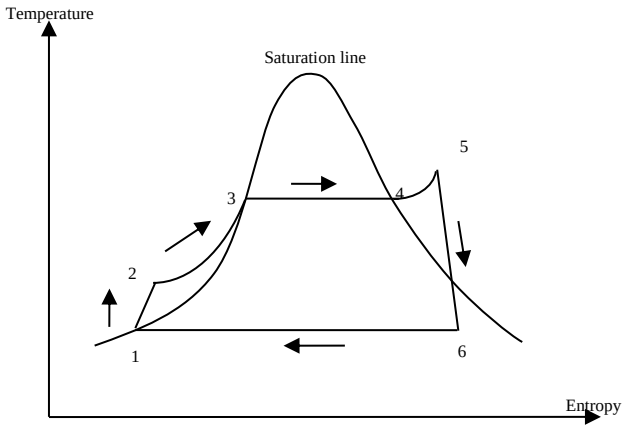

Figure 8 Mathematical Model used to describe physical processes in the Secondary Loop

3.3 Behavioral Rules and Functional Failure Logics

The BRs and FFLs of HW/SW components in the secondary loop are obtained through mathematical models simplified using qualitative physics. For example, the function of the turbine is producing electricity by consuming thermal energy. The input of the turbine is the dry saturated vapor which should be measured by flowrate, temperature, and pressure. In the nominal state, the flowrate of the input to the turbine should be equal to the flowrate of the output to the turbine, and the temperature and pressure of the output should be equal to their nominal (designed) values. Otherwise, the turbine would be in a faulty mode. The condenser's function is to condense the wet vapor to become a saturated liquid. The parameters of the inputs and outputs of a condenser should be the flowrate, temperature, pressure, and chemical density. As two examples, Table I lists the BRs and FFLs defined for the turbine and the condenser.

Table I Examples of BRs and FFLs for Critical Components

Components	Inputs	Outputs	Behavior Rules	Functional Failure Logic
Turbine	Q_{in} T_{in} P_{in}	Q_{out} T_{out} P_{out}	Mode == Nominal IF Q_{out} == Q_{in} AND T_{out} == $T_{out, nom}$ AND P_{out} == $P_{out, nom}$ Mode == Outlet Temperature High IF $T_{out} > T_{out, nom}$ Mode == Outlet Temperature Too High IF $T_{out} >> T_{out, nom}$ Mode == Outlet Pressure Low IF $P_{out} < P_{in}$ Mode == Outlet Flow Low IF $Q_{out} < Q_{in}$	IF mode == Nominal Then Energy Transformation == O IF mode == Outlet Temperature High Then Energy Transformation == D IF mode == Outlet Temperature Too High Then Energy Transformation == L IF mode == Outlet Pressure Low Then Energy Transformation == L IF mode == Outlet Flow Low Then Energy Transformation == L
Condenser	Q_{in} T_{in} P_{in} C_{in}	Q_{out} T_{out} P_{Out} C_{out}	Mode == Nominal IF Q_{out} == Q_{in} AND T_{out} == $T_{out, nom}$ AND P_{out} == P_{in} Mode == Outlet Temperature High IF $T_{out} > T_{out, nom}$ Mode == Outlet Temperature Too High IF $T_{out} >> T_{out, nom}$ Mode == Outlet Pressure Low IF $P_{out} < P_{in}$ Mode == Outlet Flow Low IF $Q_{out} < Q_{in}$ Mode == Tube Leak IF $C_{out} > C_{out, nom}$	IF mode == Nominal Then Condensate Steam == O IF mode == Outlet Temperature High Then Condensate Steam == D IF mode == Outlet Temperature Too High Then Condensate Steam == L IF mode == Outlet Pressure Low Then Condensate Steam == L IF mode == Outlet Flow Low Then Condensate Steam == L IF mode == Tube Leak Then Condensate Steam == L

Note: O, operating; L, lost; D, degraded; U, unknown; C, complete; NA, not applicable; T_{in}, input temperature; T_{out}, output temperature; P_{in}, input pressure; P_{out}, output pressure; Q_{in}, input flow rate; Q_{out}, output flow rate; C_{in}, input chemical density; C_{out}, output chemical density; Nom, nominal.

In Table I, the inputs and outputs are the parameters of in-flow and out-flow acquired from mathematical models based on qualitative physics. The BRs express all possible states of components, including the nominal and various faulty states. The FFLs denotes the conditions for reasoning on the states of functions.

3.4 Simulation Results

A great number of fault propagation data are gathered via ISFA simulations. In this section, an example of a result is interpreted. The fault injected is a pipe leak and the results are summarized in Table II. The important simulation steps are discussed in detail.

- Time step t = 1: initial state. All subsystems/components are running correctly.

- Time step t = 6: A pipe leakage fault is injected into Pipe11. This degrades the functionality of the pipe (i.e., transfer fluid). In addition, chemical coming from the leaking point enters into the steam, which causes the functionality of the pipe to further degrade. Because the software controlling the valve in case of load loss is inactive, the Turbine Bypass Valve is closed so that the steam with chemicals is cannot reach the Condenser.
- Time step t = 106: After 100 time steps (the assumed life span of Temperature Sensor1), Temperature Sensor1 fails due to the steam blowing at high temperature and pressure.
- Time step t = 120: The control software is activated by the plant operator. The Turbine Bypass Valve is opened (assume the Condenser is available, which is mostly always the case) and the steam goes through Pipe12 to the Condenser. However, due to the failure of Temperature Sensor1, the amount of sprayed water is calculated incorrectly (e.g., no cool water is provided), and the temperature and pressure outlet of the Turbine Bypass Valve is set to be higher than normal. Consequently, the high temperature/pressure steam with chemicals is dumped into the Condenser.
- Time step t = 130: The control activities associated to the loss of load is completed and the Turbine Bypass Valve is closed. But the high temperature/pressure steam with chemicals remains in the Condenser.
- Time step t = 240 to 250: The same event as t = 120 to 130 occurs once again, which lets more steam into the Condenser.
- Time step t = 3000: The load loss control software has been activated so many times that the tube in the Condenser leaks which leads to the Condenser failure finally. The failure of the condenser results in a loss of system function.

Table II An ISFA Result Table of Fault Propagation Simulation

Hardware Components and Functions														**Interface**		**SW**	**SF**
	SG	P1	P2	TV	P3	Tb	P4	Cd	…	P11	TBV	TS1	P12	I1		LL	
time	GS	TF	TF	RF	TF	TE	TF	CS	…	TF	RF	MT	TF	T1	T2		GE
1	O	O	O	O	O	O	O	O	…	O	O	O	O	IA	IA	IA	O
6	O	O	O	O	O	O	O	O	…	D	O	O	O	IA	IA	IA	O
…																	
106	O	O	O	O	O	O	O	O	…	D	O	L	O	IA	IA	IA	O
120	O	O	O	O	O	O	O	O	…	D	D	L	O	C	IA	A	O
130	O	O	O	O	O	O	O	O	…	D	D	L	O	IA	C	C	O
...																	
240	O	O	O	O	O	O	O	O	…	D	D	L	O	C	IA	A	O
250	O	O	O	O	O	O	O	O	…	D	D	L	O	IA	C	C	O
...																	
3000	O	O	O	O	O	O	O	L	…	D	D	L	O	IA	IA	IA	L

Note: Hardware Components: SG – Steam Generator, P1 – pipe 1, P2 – Pipe 2, TV – Turbine control Valve, P3 – Pipe3, Tb – Turbine, P4 – Pipe 4, Cd – Condenser, P11 – Pipe 11, TBV – Turbine Bypass Valve, TS1 – Temperature Sensor 1, P12 – Pipe 12. Interface: I1 – <<interface>> I1. Software Component: LL – Load Loss. Hardware Functions: GS – Generate Steam, TF – Transfer Fluid, RF – Regulate Fluid, TE – Transfer Energy, CS – Condense Steam, MT – Measure Temperature. Transaction: T1 – Open Turbine Bypass Valve, T2 – Close Turbine Bypass Valve. System Function: GE – Generating Energy. Function States: O – Operational, D – Degraded, L – Lost, IA – Inactive, C – Complete, A – Activated.

According to the resultant data in Table II, the fault injected into Pipe11 leads to the degradation of the TBV and the failure of TS1. Consequently, the failed TS1 provides illegal temperature values to the control software. Periodic load losses incurred in the NHES lead to frequent Open TBV/Close TBV transactions.

These actions deteriorate the work environment of the Condenser and finally damage the Condenser. The periodic transactions sent by the control software can be defined as a feature. The degradation sequence where the TBV's degradation precedes TS1's is another feature. The combination of both features can be seen as the effect of faulty Pipe11. Features are identifiable when the OLM is capable of observing the transactions, the states of the TBV, and the signals from TS1. Identifiable features are utilized to distinguish faults. By injecting different faults into the system, the degree of the contribution to fault identification $I_j(OS_i)$ can be calculated for each observable signal OS_i. If all values of $I_j(OS_i)$ related to the faulty Pipe11 are greater than zero, the fault is identifiable by the OLM system. Otherwise, the OLM system is incapable of fault identification. To enhance the fault detection capability, DCOs of unobservable signals are required to determine which signals should be observed preferentially. The DCOs can be calculated via equation (4). Suppose that the transaction T1 (treated as a signal) sent by the control software is currently unobservable and that the DCO of T1 is greater than that of other signals. As a consequence, a virtual sensor (probably a probe program) will be added into the control software to optimize the OLM design. In this case, T1 is becoming an observable signal and the fault simulation and design optimization process will be executed iteratively.

4 CONCLUSION

In this paper, a methodology associated with fault analysis was introduced to design an OLM system. To improve the reliability of a secondary loop system embedded in a NHES, the methodology was defined including the acceptance criteria that determine whether the OLM system meets requirements set by the developer, the construction of models required to perform fault simulation, the simulation process associated with fault injection criteria, the method of identification of fault features, and the procedure of optimization for the OLM design. In this research, the fault propagation analysis was accomplished by applying ISFA to the secondary loop of a nuclear power plant, including the investigation of mathematical models, the creation of ISFA models of system components, functions, the definition of the behavioral rules and functional failure logic, and the execution of iterative fault simulations.

In the future, the database (which contains identifiable faults with their features) will be updated to include information for faults diagnosis online. A prototype of the OLM system for the secondary loop will be implemented by applying the proposed method to its design.

5 ACKNOWLEDGMENTS

This work was funded by the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

6 REFERENCES

1. H. Li, S. Bragg-Sitton, and C. Smidts, "failure diagnosis for the holdup tank system via ISFA," *ANS Winter Meet. Nucl. Technol. Expo*, **vol. 115**, pp. 881–884, (2016).
2. D. J. T. Siyambalapitiya and P. G. McLaren, "Reliability improvement and economic benefits of online monitoring\nsystems for large induction machines," *IEEE Trans. Ind. Appl.*, **vol. 26**, no. 6, pp. 1018–1025, (1990).
3. Z. Qiang, M. Li, and J. R. Bolton, "Development of a tri-parameter online monitoring system for UV disinfection reactors," *Chem. Eng. J.*, **vol. 222**, pp. 101–107, (2013).
4. S. D. J. McArthur, S. M. Strachan, and G. Jahn, "The design of a multi-agent transformer condition monitoring system," *IEEE Trans. Power Syst.*, **vol. 19**, no. 4, pp. 1845–1852, (2004).
5. M. L. Massie, B. N. Chun, and D. E. Culler, "The ganglia distributed monitoring system: Design,

implementation, and experience," *Parallel Comput.*, **vol. 30**, no. 7, pp. 817–840, (2004).

6. C. Mutha, D. Jensen, I. Tumer, and C. Smidts, "An integrated multidomain functional failure and propagation analysis approach for safe system design," *Artif. Intell. Eng. Des. Anal. Manuf.*, **vol. 27**, no. 4, pp. 317–347, (2013).
7. I. Tumer and C. Smidts, "Integrated design-stage failure analysis of software-driven hardware systems," *IEEE Trans. Comput.*, **vol. 60**, no. 8, pp. 1072–1084, (2011).
8. C. Mutha and C. Smidts, "An early design stage UML-based safety analysis approach for high assurrance software systems," *13th IEEE Int. Symp. High Assur. Syst. Eng. HASE 2011*, pp. 202–211, (2011).
9. H. Abdi and L. J. Williams, "Principal component analysis," *Wiley Interdisciplinary Reviews: Computational Statistics*, **vol. 2**, no. 4. John Wiley & Sons, Inc., pp. 433–459, (2010).
10. B. F. Tchanche, G. Lambrinos, A. Frangoudakis, and G. Papadakis, "Low-grade heat conversion into power using organic Rankine cycles - A review of various applications," *Renew. Sustain. Energy Rev.*, **vol. 15**, no. 8, pp. 3963–3979, (2011).