A Benchmark System for the Assessment of Reliability Modeling Methods for Digital Instrumentation and Control Systems in Nuclear Plants

J. Kirschenbaum[1], M. Stovsky[2], D. Mandelli[2], P. Bucci[1], T. Aldemir[2], D. W. Miller[2], E. Ekici[3], S. A. Arndt[4]

[1]*The Ohio State University, Dept. of Computer Science & Engineering, 2015 Neil Ave., Columbus, OH, 43210*
[2]*The Ohio State University, Nuclear Engineering Program, 201 West 19th Avenue, Columbus, OH 43210*
[3]*The Ohio State University, Dept. of Electrical & Computer Engineering, 2015 Neil Ave., Columbus, OH, 43210*
[4]*U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, D.C. 20555*

Abstract – *This paper presents a candidate system for use as a benchmark in the assessment of methods for the reliability modeling of digital instrumentation and control (I&C) systems. The system specification is based closely on a steam generator feedwater control system in an operating pressurized water reactor. Several failure scenarios that demonstrate the benchmark system's ability to address the features of loosely control-coupled digital I&C systems are discussed.*

I. INTRODUCTION

In nuclear power plants, there is an accelerating trend to upgrade and replace analog instrumentation and control (I&C) systems with digital I&C systems. This transition from analog to digital I&C systems is due to the potential of digital I&C systems to improve reliability and safety of the plants [1]. As this replacement process continues, one or more methods addressing digital I&C system reliability are needed to quantify the change in the core damage frequency and large early release frequency of the plants by such systems [2]. For the near future, the digital system models must be able to interface with current probabilistic risk assessments (PRAs) which generally use a static event tree/fault tree approach. Conversely, the models must be able to use data that was produced by a conventional PRA. A review of literature in this area appearing in NUREG/CR-6901, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments [3] has identified several methods related to digital I&C system reliability modeling [4-19] and a characterized the requirements of such a risk model [20].

A conclusion of NUREG/CR-6901 [3] is that there is no benchmark system available to be used as the basis for an objective comparison of methods for digital I&C system reliability modeling. Recently, requirements for such a benchmark have been proposed [21] based on the interactions within the digital I&C system and the interactions of the I&C system with the controlled/ monitored process. This paper presents the specifications for a benchmark system that meets the loosely control-coupled (LCC) system requirements of [21] shown in Table 1. For LCC digital I&C systems, there is no direct dependency among different processes occurring among the system constituents, including software/ firmware. However, these systems may include dependencies through the controlled/monitored process.

TABLE I. The LCC Requirements of [21] Satisfied by the Benchmark System

1	A clock which regulates information sampling from the controlled/monitored process,
1.1	regulates measurements,
1.2	may lead to roundoff,
1.3	may lead to truncation.
2	Explicit representation of the power requirements that are needed for the digital systems including
2.1	loss of power,
3	Real-time constraints
4	A polling capability with
4.1	events occurring in between polls,
4.2	sensors that are being polled failing to report a value
5	An interrupt capability with
5.1	interrupts occurring at an excessive rate,
6	Long term storage with
6.1	failures that can occur in the retrieval of information,
6.2	failures that can occur in the saving of information,
6.3	Loosely-Coupled Requirement 3.
7	Computation capability both based on the controlled/monitored process physics and interacting with the process physics
7.1	stimulates interaction with the physical process
7.2	can produce intermittent and functional failures
8	A self-diagnostic system where
8.1	contradictory data can be delivered to the system,
8.2	events can occur while in self-diagnostic mode.
9	A watchdog timer with
9.1	instances in which there is no safe state, instances in which the watchdog timer fails.

II. BENCHMARK SYSTEM

The benchmark system is based upon the steam generator (SG) feedwater system of an operating 2-loop pressurized water reactor (PWR). Each loop has its own digital feedwater controller (DFWC). Section II.A provides a high level description of the benchmark system. Section II.B describes the connections among system hardware devices. Section II.C states the control laws. Section II.D lists the fault tolerant features of the benchmark system. Section III describes two scenarios that demonstrate the benchmark system's ability to fulfill many of the LCC requirements.

II.A. High Level Description of Benchmark System

The purpose of the DFWC is to maintain the water level inside each of the SGs optimally within ± 2 inches of the setpoint level (defined at 0 inches). The overall DFWC system configuration for Loop 1 is shown in Fig.1. The DFWC is connected to a feedwater pump (FP), a main feedwater regulating valve (MFV), and a bypass feedwater regulating valve (BFV). The control algorithms are executed on both a main computer (MC) and backup computer (BC). These computers produce demand signals (σ_{B1}, σ_{M1}, σ_{F1}) for the MFV, BFV, and FP. The selection of the appropriate signal to be used from the MC and BC for each of these actuated devices ($\widetilde{S}_{B1}, \widetilde{S}_{M1}, \widetilde{S}_{F1}$) is determined by a controller. Each of the controllers may forward the MC or BC's outputs to the device to which it is connected, or it may maintain the previous output to that device. Another controller, the PDI controller (pressure differential indicator controller), serves as a backup for the MFV controller. The PDI controller reads the value of the signal originating from the MFV controller. If the MFV controller fails to send a signal, the PDI will reproduce the most recent value of the signal on the MFV controller's output to the MFV. The PDI is also connected to the BFV, MFV, and FP controllers to share status information.

Under normal conditions, the feedwater control system operates in different modes depending on the power generated in the primary system. These modes are the following:

1 Low power automatic mode
2 High power automatic mode
3 Automatic transfer from low to high power mode
4 Automatic transfer from high to low power mode

The low power mode of operation occurs when the reactor operates between 2% and 15% reactor power. In this mode, the BFV is used exclusively to control the feedwater flow. The MFV is closed and the FP is set to a minimal value. The control laws (see Section II.C) use the feedwater flow rate (f_{w1}), the steam flow rate (f_{s1}), feedwater temperature (h_{w1}), feedwater level in the steam generator (x_1), and neutron flux (P) to determine the BFV position. The feedwater level is fed to a proportional-integral (PI) controller algorithm using the feedwater temperature to determine the gain. Then this value is summed with the feedwater flow and neutron flux.

High power mode is used when the reactor is operating between 15% and 100% reactor power. In this mode, the MFV and the FP are used to control the feedwater flow. The BFV is closed in a manner that is similar to the MFV in low power mode. The control laws (see Section II.C) again use f_{w1}, f_{s1}, h_{w1}, x_1 and P to compute the total feedwater demand. This computed value is used to determine both the position of the MFV and the speed of the FP. The feedwater flow and steam flow are summed and fed to a set of PI controller algorithms. The output from these controller algorithms is added to the feedwater level and that result is fed to a PI controller algorithm that uses the steam flow for the controller's gain.

Transitions between low and high power are controlled by the neutron flux readings. When the system is in low power mode and the neutron flux increases to a point when high power mode is necessary, the MFV is signaled to open while the BFV is closed to maintain needed feedwater flow. The opposite transition occurs when the system is in high power mode and the neutron flux decreases to a point when low power mode is needed.

The controller is regarded failed if water level in a SG rises above +30 or falls below -24 inches.

II.B. Benchmark System Connections

The sensor signals are routed to provide information to both the main and backup computers as shown in Fig. 2 and 3. Setpoint data changes are delivered from the MFV controller to the MC and BC through an analog signal.

The digital feedwater controller components are connected together in several different ways. The MC and BC both connect to the MFV, BFV, and FP controllers through an analog control signal and failure status signals. The MFV, BFV, and FP controllers are connected so they may share status information.

II.C. Benchmark System Control Laws

The control laws for the system under normal operating conditions are as follows:

Rate of Level Change:

$$\frac{dx_1}{dt} = A\left(f_{wn} - f_{sn}\right) \qquad (1)$$

Flow Demand (C_{Fn})

$$C_{Fn}(t) = \beta_{Fn}(f_{sn})^* \int dt[\rho_n - C_{\ln}(t) + E_{Fn}(t)] - \lambda_{Fn}(\sigma_{Bn}) \quad (2)$$

Compensated Water Level (C_{ln})

$$\tau_2 \frac{dC_{ln}}{dt} = -C_{\ln} + x_n + \tau_1(f_{wn} - f_{sn}) \quad (3)$$

Compensated Flow Error (E_{Fn})

$$\tau_5 \frac{dE_{Fn}(t)}{dt} + E_{Fn}(t) = \tau_7 \left[\frac{df_{wn}}{dt} - \frac{df_{sn}}{dt} \right] \quad (4)$$

Compensated Power (C_{pn})

$$\tau_4 \frac{dC_{pn}}{dt} = -C_{pn}(t) + p_n + \tau_3 \frac{dp_n}{dt} \quad (5)$$

BFV Demand (C_{Bn})

$$C_{Bn}(t) = \upsilon_{Bn}\alpha_M + \upsilon_{Bn}C_{pn}(t) + \beta_{Bn}(h_{wn}) \int dt[\rho_n - C_{\ln}(t)] - \lambda(\sigma_{Mn}) \quad (6)$$

In Eqs.(1)-(6), ρ_n is the level setpoint for SGn (n=1,2), p_n is the power level of SGn, υ_{Bn}, α_M, A and τ_1 - τ_7 are user-specified constants. The $\lambda_{Fn}(\sigma_{Bn})$, $\beta_{Fn}(f_{sn})$ and $\beta_{Bn}(h_{wn})$ are obtained from lookup tables.

The MFV demand in high power is determined by Eq.(2). At low power, MFV demand is zero. At high power, the BFV demand is zero. At low power, the BFV demand is determined by Eq.(6). The FP demand at high power is determined by the maximum of the flow demands of MFVs for both Loop 1 and 2. At low power, it is set to a constant value. The user-specified constants (e.g., the τ_1 - τ_7) are stored in a flash drive in both the MC and BC. The f_{wn} and f_{sn} in Eq.(2) are determined from the steam generator model of [5].

II.D. Fault Tolerant Features of Benchmark System

The benchmark system has a number of fault tolerant features:

a) Because the MFV, BFV, and FP controllers forward the control signals to the corresponding control points (the MFV, BFV, and FP, respectively), they provide a level of fault tolerance if both computers fail by allowing the operators time to intervene by holding the outputs of each to a previously valid value.
b) The computers, MFV and BFV and FP, and PDI controllers are each connected to an independent power source wired to a separate bus. A single power source failure can only affect one computer, all of the MFV/BFV/FP controllers, or the PDI controller at one time.
c) Both the MC and BC are set to oversample at 3 times the Nyquist criterion to avoid aliasing.
d) The computers are able to process the sensor inputs and perform the control algorithms within one third of the needed response interval of the physical process. A failure in the MC or BC can be detected and the fail over to a healthy component can occur with enough time to meet the response requirements of the process.
e) The water level setpoint is taken from a switch connected to the MFV and is propagated to all computers. If the setpoint signal goes out of range, then the computers fall back to a preprogrammed setpoint value.
f) Each computer is connected to a watchdog timer. A watchdog timer is a hardware timer and associated connections used to determine if a software error or other computer failure has rendered a processor unusable. In general, a normally functioning computer resets the watchdog timer at regular, defined intervals so the timer does not “go off.” However, in the presence of a software error or other computer failure, the timer will not be reset by the computer and the timer can go off. If the timer goes off, all components in the controller connected to the watchdog timer are notified of the computer failure. In the case of the benchmark system, the MFV, BFV, and FP controllers are notified and transfer control away from the affected computer.
g) Each computer verifies and validates its inputs, checking for out of range and excessive rate changes in the inputs that would indicate errors in the sensor readings or problems with the analog to digital conversion of the values. Each computer ignores input that fails these checks if the other inputs are still valid.
h) The values of the inputs are averaged across redundant sensors.

i) Deviation between the two sensors is detected and, if the deviation is large enough, the computer can signal a deviation error to the MFV, BFV, and FP controllers so they may switch to another computer.
j) The PDI controller provides one more level of fault tolerance, in that it holds the MFV at the current position if the MFV does not produce output.
k) The MFV, BFV and FP controllers also send their outputs to the MC and BC. When the MC (or BC) is in control, it compares its output to the signals that the MFV, BFV and FP controllers output signal to the actuators. If the output signal differs, then the computer indicates to the MFV, BFV and FP controllers that it has failed..

The DFWC fail over logic consists of the following: The MC has control of the control points initially, with the BC in hot standby. If the MC fails, then the BC takes control. If the BC fails after the MC has failed, then the MFV, BFV, and FP controllers each use a recent output value from the computer (essentially the last one that the controller can store) and propagate that value to the control points. Any time a component fails, the operator console is notified to allow operators to take mitigating actions.

III. EXAMPLE FAILURE SCENARIOS FOR THE BENCHMARK SYSTEM

These scenarios were created to demonstrate the ability of the benchmark system to exercise reliability methodologies according to the LCC requirements and the ability to portray possible scenarios that may occur in nuclear power plants. These scenarios were created based upon the literature available on possible failure scenarios [22, 23].

III. A. Scenario 1

The scenario starts with the benchmark system operating at high power at 90% reactor power with the MC controlling the MFV, BFV, and FP, the BC operating correctly and the MFV, BFV, FP, and PDI controllers operating correctly. When the FP controller was installed, the MC to FP and BC to FP failure signal wire were not soldered correctly [23]. As a result of the improper soldering and vibration within the plant, the integrity of these connections has become compromised. Additionally, as has been encountered in operating nuclear power plants [22], corrosion problems have affected the wiring. In this scenario, the corrosion affects one of the water level sensor wires from level sensor 1 (LVL1) (see Fig.1 and 2). As a consequence of the corrosion, the MC receives intermittently no signal from LVL1 over the course of several months.

Due to wear-out affecting the connection from level sensor 2 (LVL2), the sensor is unable to transmit a signal and fails to report a value (resulting in 0.0 DC volts on the line). The MC senses this signal loss and ignores the invalid input.

At this point, corrosion in the connection from LVL1 described above causes the connection to fail completely, resulting in 0.0 DC volts on the line. Consequently, no signal is received by the MC from LVL1.

At this point, all level sensor transmissions to the MC have failed. The MC waits for one processing cycle, determines the level sensor inputs are still unavailable and then signals failure to the MFV, BFV, and FP controllers. As a result of the MC failure, the MFV, BFV, and FP controllers each attempt to transfer control to the BC.

Due to vibration, the FP controller's MC and BC failure status wires become completely disconnected from the controller. This disconnection causes the FP controller to consider both the MC and BC as failed. By following its fail over procedure, the FP controller recycles its last good output. The FP controller then signals MC and BC failure to the MFV and BFV controllers. This causes the MFV and BFV controllers to recycle their last good outputs until operators intervene.

Table II. Summary of Scenario 1

Preconditions for Scenario 1
Scenario 1
1. Level sensor two fails due to a broken connection.
2. Level sensor one fails as the corrosion causes the wire to degrade too much to be usable.
3. MC activates failure status signal.
4. MFV, BFV, and FP controllers transfer control to the BC.
5. MC to FP and BC to FP controller failure status lines become disconnected due to vibration.
6. FP signals BC and MC failure to other controllers and uses last good output value.
7. MFV and BFV controllers use last good output

Scenario 1 is summarized in Table II. This scenario demonstrates the benchmark system can fulfill the benchmark requirements 4, 7, and 8. Namely the benchmark system interacts with a physical process and can include both intermittent and functional failures. The

benchmark system includes polling sensors which may or may not return a value, and a self-diagnostic system that can have inconsistent data delivered to it.

III.B. Scenario 2

Scenario 2 starts with the system operating normally in high power at 90% reactor power with the MC in control and all other controllers and components operating normally.

The BC fails and causes the watchdog timer to expire. This timer expiration is detected as BC failure by the MFV, BFV, and FP controllers.

Due to corrosion of an inline power supply fuse, the power supply to the MC shuts down [22, 23], resulting in an MC failure. The MFV, BFV, and FP controllers detect the loss of the MC and take control holding the valves and pumps settings at their current values until operators are able to intervene.

Table III. Summary of Scenario 2

Preconditions for Scenario 2
1. Corrosion of an inline power supply fuse to MC.
Scenario 2
1. BC fails. 2. BC's watchdog timer expires. 3. MC power supply fails. 4. MC fails. 5. MFV, BFV, and FP controllers take control and maintain pumps/valve settings at current values until operators intervene.

Scenario 2 is summarized in Table III. This scenario demonstrates the benchmark system's ability to fulfill requirements 2 and 9, namely the representation of electrical power needs and the use of the watchdog timer.

IV. CONCLUSIONS

A DFWC system similar to that of an operating 2-loop PWR is proposed as benchmark system for assessing the capabilities of methods for the reliability modeling of digital I&C systems. Two scenarios have been presented to demonstrate the ability of the benchmark system to fulfill some of the LCC requirements of [21] and to show the benchmark systems ability to represent a rich class of failure scenarios that have been based upon accident reports. Additional scenarios will be developed to fulfill the remaining requirements for the LCC benchmark.

ACKNOWLEDGMENTS

The research presented in this paper was sponsored by the U.S. Nuclear Regulatory Commission (US NRC). The information and conclusions presented here in are those of the authors and do not necessary represent the views or positions of the US NRC. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assume any legal liability or responsibility for any third party's use of this information.

REFERENCES

[1] Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades - Applying Risk-Informed and Deterministic Methods, 1002835, EPRI, Palo Alto, CA (2004)

[2] ADVISORY COMMITTEE ON REACTOR SAFEEGUARDS, *Regulatory Guidance on Implementation of Digital I&C Systems* (1997).

[3] T. ALDEMIR, D. W. MILLER, M. STOVSKY, J. KIRSCHENBAUM, P. BUCCI, A. W. FENTIMAN, and L. A. MANGAN, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, U. S. Nuclear Regulatory Commission, Washington, D.C. (2006)

[4] C. J. GARRET and G. E. APOSTOLAKIS, "Automated Hazard Analysis of Digital Control Systems", *Reliab.Engng & System Safety,* **77**, 1-17 (2002).

[5] S. GUARRO, M. YAU, and M. MOTAMED, Development of Tools for Safety Analysis of Control Software in Advanced Reactors, NUREG/CR-6465, U.S. Nuclear Regulatory Commission, Washington, D.C. (1996)

[6] D. T. SMITH, T. A. DELONG and B. W. JOHNSON, "A Safety Assessment Methodology for Complex Safety-Critical Hardware/Software Systems", *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Washington, D.C. (2000).

[7] N. F. SCHNEIDEWIND and T. W. KELLER, "Applying Reliability Models to the Space Shuttle", *IEEE Software*, 28-33 (1992).

[8] Y. ZANG and M. M. GOLAY, "Development of a Method for Quantifying The Reliability of Nuclear Safety-Related Software", *PSAM6: Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management, CD-ROM Version*, Elsevier Science Ltd. (2002).

[9] G. PAI, S. DONOHUE and J. DUGAN, "Estimating Software Reliability From Process and Product Evidence", Elsevier Science Ltd. (2002).
[10] P. L. GODDARD, "A Combined Analysis Approach to Assessing Requirements for Safety Critical Real-Time Control Systems", *IEEE Proceedings Annual Reliability Maintainability Symposium*, Hughes Aircraft Company (1996).
[11] A. RAUZY, "Mode Automata and Their Compilation into Fault Trees", *Reliab.Engng & System Safety*, **78**, 1-12 (2002).
[12] BALAKRISHMAN, M. and K. TRIVEDI, "Stochastic Petri Nets for Reliability Analysis of Communication Network Applications With Alternate Routing", *Reliab.Engng & System Safety*, **53**, 243-259 (1996).
[13] J. L. PETERSON, "Petri Nets", *ACM Computing Surveys*, **9** (1977).
[14] M. MARSAN and G. CONTE, "A Class of Generalized Stochastic Petri Nets for the Performance Evaluation of Multiprocessor Systems", *ACM Transactions on Computer Systems*, **2**, 93-122 (1984).
[15] T. S. LIU and S. B. CHIOU, "The Application of Petri Nets to Failure Analysis", *Reliability Engineering and System Safety*, 129-142 (1997).
[16] B. LI, M. LI and C. SMIDTS, "Integrating Software into PRA: A Test-Based Approach", C. SPITZER, U. SCHMOKER and V. N. DANG (Eds.), Springer – Verlag, London, U.K. (2004).
[17] C. SMIDTS and M. LI, Validation of A Methodology For Assessing Software Quality, UMD_RE_2002-07, University of Maryland, College Park, MD, (2-1-2002)
[18] N. F. SCHNEIDEWIND, "Analysis of Error Processes in Computer Software", *Proc.Int'l Conf.Reliable Software*, 76-78, IEEE CS Press (1975).
[19] L. M. KAUFMAN and B. W. JOHNSON, Embedded Digital System Reliability and Safety Analyses, NUREG/GR-0020, U.S. Nuclear Regulatory Commission, Washington, D.C. (2001)
[20] S. A. ARNDT, E. THORNSBURY and N. O. SIU, "What PRA Needs From a Digital System Analysis", E. J. BONANO, A. L. CAMP, M. J. MAJORS and R. A. THOMPSON (Eds.), *Probabilistic Safety Assessment and Management*, Elsevier Science Publishing Co., New York (2001).
[21] J. KIRSCHENBAUM, M. STOVSKY, P. BUCCI, T. ALDEMIR and S. A. ARNDT, "Benchmark Development for Comparing Digital Instrumentation and Control System Reliability Modeling Approaches", American Nuclear Society, LaGrange Park, IL (2005).
[22] J. K. KIRKWOOD, Reactor Trip Due to Low Steam Generator Water Level After Feed Pump Trip, 2004-01-00, (3-23-2004)
[23] Technical Specification Non-Compliance Due to Loose Wire on a HPCI System Valve Logic Relay, 4-03-0, (2006)

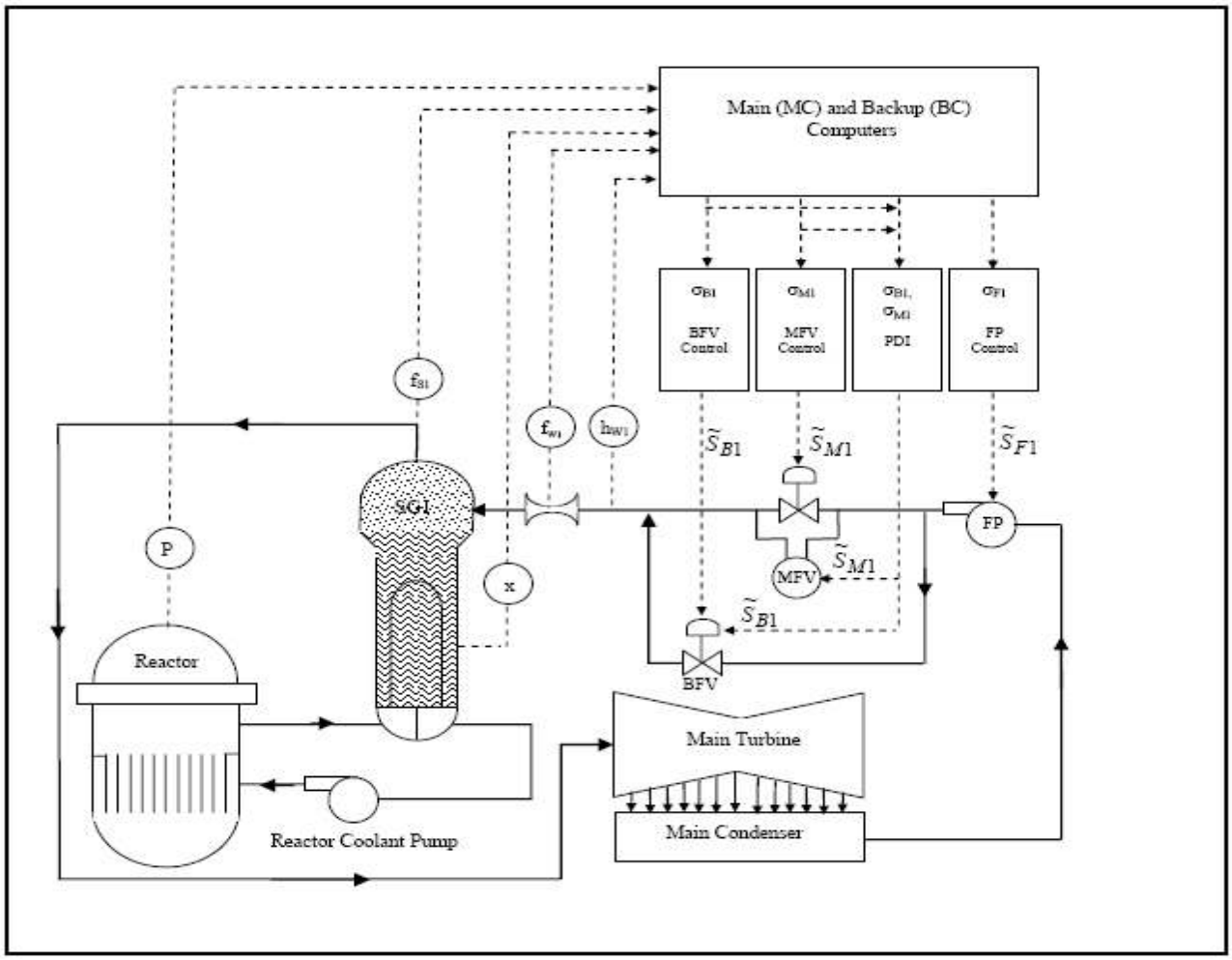

Fig. 1. Detailed View of the Benchmark System

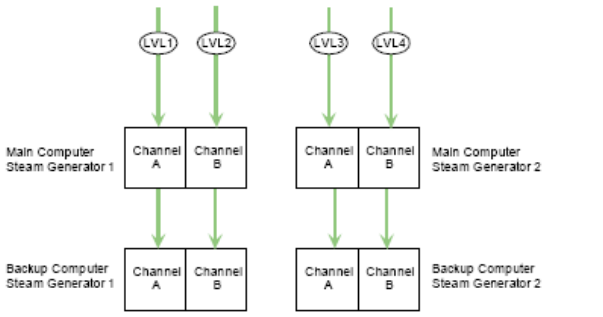

Fig. 2. Example Sensor Connection With 4 Physical Sensors

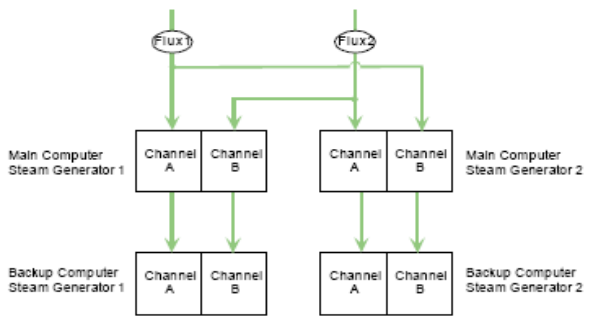

Fig. 3. Example Sensor Connection With 2 Physical Sensors