FINAL PROGRESS REPORT

DE-NE0000739

Advanced I&C for Fault-Tolerant Supervisory Control of Small Modular Reactors

University of Pittsburgh

PI: Dr. Daniel G. Cole
Associate Professor
Director of Nuclear Engineering
dgcole@pitt.edu
412-624-3069

Project period of performance:
01/27/2014–10/31/2017

Reporting period:
01/27/2014–10/31/2017

Rev. 0
2018-01-31

Summary

In this research, we have developed a supervisory control approach to enable automated control of SMRs. By design the supervisory control system has an hierarchical, interconnected, adaptive control architecture. A considerable advantage to this architecture is that it allows subsystems to communicate at different/finer granularity, facilitates monitoring of process at the modular and plant levels, and enables supervisory control. We have investigated the deployment of automation, monitoring, and data collection technologies to enable operation of multiple SMRs. Each unit's controller collects and transfers information from local loops and optimize that unit's parameters. Information is passed from the each SMR unit controller to the supervisory controller, which supervises the actions of SMR units and manage plant processes. The information processed at the supervisory level will provide operators the necessary information needed for reactor, unit, and plant operation.

In conjunction with the supervisory effort, we have investigated techniques for fault-tolerant networks, over which information is transmitted between local loops and the supervisory controller to maintain a safe level of operational normalcy in the presence of anomalies. The fault-tolerance of the supervisory control architecture, the network that supports it, and the impact of fault-tolerance on multi-unit SMR plant control has been a second focus of this research. To this end, we have investigated the deployment of advanced automation, monitoring, and data collection and communications technologies to enable operation of multiple SMRs. We have created a fault-tolerant multi-unit SMR supervisory controller that collects and transfers information from local loops, supervise their actions, and adaptively optimize the controller parameters.

The goal of this research has been to develop the methodologies and procedures for fault-tolerant supervisory control of small modular reactors. To achieve this goal, we have identified the following objectives. These objective are an ordered approach to the research: I) Development of a supervisory digital I&C system II) Fault-tolerance of the supervisory control architecture III) Automated decision making and online monitoring.

Contents

Chapter 1

Goal and Objectives

The purpose of this research has been to develop advanced instrumentation and control (I&C) techniques for improved supervisory control relevant to the operational goals of small modular reactors (SMRs). A significant challenge for making viable SMRs is the need to reduce demands for labor-intensive surveillance, testing, and inspection. In this research, we have used to use advanced control techniques to enable automated online, in-situ monitoring of SMR I&C components. This would allow engineers to rapidly measure system dynamics and loop processes, and tune these loops to optimize conditions for peak performance. A significant advantage would be that these tools can be used during reactor operation to monitor components. In this research, we have also investigated techniques for fault-tolerant networks. The I&C system would have an interconnected, hierarchical control architecture, allowing subsystems and SMR units to communicate. To ensure that proper monitoring, safety, and control of reactor and plant processes are maintained, a fault-tolerant communication network must be maintained.

1.1 Research Description

The vision for small modular reactors (SMRs) goes beyond large single-unit power generation to multiple smaller units at one site supplying steam to a turbine and the possibility of steam co-generation for industrial needs.[1,2,3] The challenge for multi-unit operation is twofold: First, staffing needs must be addressed since this is seen a necessary for the economic viability of the concept.[1,3] While many plant operations must be overseen by human operators, there will likely need to be an increased level of automation in SMR operations.[4,5] This will be particularly so for control functions, which must maintain suitable margins from safety limits during plant transients, versus safety functions, which must maintain a certain level of operator interaction in order to meet regulatory safety requirements.

Second, while each unit is independent from other units with respect to steam generation, the combination of multiple units feeding a single turbine or co-generation processes functionally ties these units together.[6] Considerations for each unit's operation must be accounted for with respect to processes in the balance of plant and overall plant economics.[3] SMRs likely will not be asked to provide base load but instead must provide load following. The economic considerations for load following can result in complicated economic dispatch models that also must account for operational considerations (e.g., unit start-up or xenon transients during shutdown.)[1] While well-known algorithms for economic dispatching[7] can be used to manage a multi-unit SMR site, start-up and shutdown increase operator workload, and some tasks (e.g., bringing a reactor critical) should demand operator action, even if only to provide permission[1].

The challenge is to find the correct balance between computer control and operator control. The objective is to have the computer maintain control over those tasks and processes that are tedious or trivial (e.g., rod control) and have the operator maintain control over plant objectives. The use of automatic control to control temperature and level setpoints has been well established in the nuclear industry. Three things are needed to meet these challenges: First, a system control architecture that allows controller parameters to be adjusted as necessary to meet changing operating conditions for multiple SMR units in a timely fashion. Second, a supervisory control strategy that allows units to be maneuvered independently to meet changing grid conditions, load following, and plant transients. Third, the system of SMR modules, balance of plant, and supervisory controller must be fault-tolerant to minimize the effects of failures on plant operation and safety.

In this research, we have developed a supervisory control approach to enable automated control of SMRs.[8] By design the supervisory control system has a hierarchical, interconnected, adaptive control architecture. A considerable advantage to this architecture is that it allows subsystems to communicate at different/finer granularity, facilitates monitoring of process at the modular and plant levels, and enables supervisory control. We have investigated the deployment of automation, monitoring, and data collection technologies to enable operation of multiple SMRs. Each unit's controller collects and transfers information from local loops and optimize that unit's parameters. Information is passed from the each SMR unit controller to the supervisory controller, which supervises the actions of SMR units and manage plant processes. The information processed at the supervisory level will provide operators the necessary information needed for reactor, unit, and plant operation.

In conjunction with the supervisory effort, we have investigated techniques for fault-tolerant networks, over which information is transmitted between local loops and the supervisory controller to maintain a safe level of operational normalcy in the presence of anomalies. The fault-tolerance of the supervisory control architecture, the network that supports it, and the impact of fault-tolerance on multi-unit SMR plant control has been a second focus of this research. To this end, we have investigated the deployment of advanced automation, monitoring, and data collection and communications technologies to enable operation of multiple SMRs. We have created a fault-tolerant multi-unit SMR supervisory controller that collects and transfers information from local loops, supervise their actions, and adaptively optimize the controller parameters.

1.2 Research Objectives

The goal of this research has been to develop the methodologies and procedures for fault-tolerant supervisory control of small modular reactors. To achieve this goal, we have identified the following objectives. These objective are an ordered approach to the research.

I. *Development of a supervisory digital I&C system*:

   In this objective, we have developed an interconnected, hierarchical, supervisory control architecture. This allows control processes to operate at the local level and adapt controllers for each unit to meet that unit's operating mode. The supervisory controller has the following functions:[1]

   - Monitor plant conditions and coordinate the appropriate operating modes for each unit's control systems.
   - Establish the each unit's power reference signal. The power reference signal will be used to derive reference and feedforward signals for the SMR control loops.

II. *Fault-tolerance of the supervisory control architecture*:

The items above can be more easily accomplished when the environment is fault-free; otherwise, redundancy must be built into the algorithms and hardware, making it more difficult for verification and validation. To achieve the desired fault tolerance for supervisory control, we have architected fault tolerance at the various levels of supervisory control, starting with redundant ECUs (embedded control units) whereby each local loop is resilient in and of itself. Through a wireless backup network, local loops are ensured that their messages will be both sent and received by the unit controllers. This redundancy is needed due to the variety of failures that can occur in such networks, especially in a nuclear environments. Similarly, the unit controllers will have ensured delivery of messages (both sent and received) from the supervisory controller, with the wireless and wired networks co-existing. We will study both node and link failures, for both correlated and independent faults.

III. *Automated decision making and online monitoring*:

In this objective, we have developed new methods to meet demands in SMR control and safety decision making. This is realized by not only monitoring system signals, but by comparing them against models of the system used by the supervisory controller. The benefit is that the reactor operator (RO) and plant engineers will be better able to estimate margins between operating parameters and design parameters. The challenge is to determine the proper balance between direct operator control and computer control of SMR and plant processes.

The remainder of this report outlines the accomplishments for each of these objectives.

Chapter 2

Development of a supervisory digital I&C system

2.1 Supervisory Control System

By design the supervisory control system has a hierarchical, interconnected, feedback control architecture. A considerable advantage to this architecture is that it allows subsystems to communicate at different/finer granularity, facilitates monitoring of process at the modular and plant levels, and enables supervisory control. Each module's controller collects and transfers information from local loops. Information is passed from each SMR unit to the plant controller, which coordinates the actions of each module and manages plant processes. The information processed at the master level provides operators the necessary information needed for reactor, module, and plant operation.

2.1.1 Functions

Fundamental Functions

Power generation in the SMRs must be closely monitored in order to ensure the integrity of the reactor modules. The removal of heat from the plant system occurs at the energy sinks, and at steady state energy generation must equal energy removal. Energy levels in each module and throughout the plant must be monitored and controlled so that temperatures do not exceed safety limits. To this end, and as stipulated in Cetiner et al. [9], the supervisory control system perform three fundamental functions:

1. *Monitor heat generation rate*: Heat is generated primarily in the reactors. The power of the reactor is monitored in two ways: First, the enthalpy increase across the reactor can be determined from temperature and pressure measurements at the reactor's inlet and outlet. Second, in-core neutron flux measurements provide a secondary measure of reactor power. Both measurements are used in control schemes that regulate the reactor power. In addition, and adjunct to this fundamental function, the temperature of the salt coolant must be monitored.

2. *Monitor heat removal rate*: Heat is removed by various sinks: Gas power Brayton cycles are used in this research for generation of electricity. Process heat provides a second energy sink. Finally, cooling towers provide one option for an ultimate heat sink in the event that power generation and process heat are unavailable. Because a salt vault is used in this plant configuration, it is not required that there be a strict energy balance at all times. Some energy generated by the reactors can be accumulated in the salt vault. Even so, the removal of heat must be monitored and match energy generation plans.

3. *Govern heat flow*: The heat flow from the reactor to the turbines must be governed. At steady state the heat transfer into and out of each loop must be equal. The primary, secondary, and power cycle loops all have sufficiently small energy storage capability that each loop must operate so that, even during transients, an energy balance must be maintained between the input and output. The salt vault, part of a tertiary loop, is an energy accumulator and by design can store large amounts of energy; thus, the energy balance for the salt vault at any point in time need not be zero. Even so, the particular operating state of the salt vault must be monitored and match requirements and prescription for economic dispatch of the plant.

Support Functions

Support functions of the supervisory controller include supervising and managing plant operations, maximizing the economy of the plant, proposing alternate operation strategies based upon system health, multi-module management, load allocation, mode transitions, optimized plant performance, diagnosis and health monitoring.

- *Supervising and managing plant operations*: This function is self evident, and is the aggregate of the other functions listed in this section.

- *Maximizing the economy of the plant*: This function relies upon effective economic dispatch of the plant. With multiple modules and uses for the heat, the economy of the plant can depend strongly on the particular combination of the energy source and energy sinks. Common economic dispatch models relate instantaneous power to generation cost; however, the use of the salt vault complicates this relationship, requiring the consideration of the power generation history and its affect on cost.

- *Proposing strategies based on health*: Failures in plant subsystems can necessitate the plant operating in a degraded mode. Some faults can be tolerated, and techniques for handling them are designed into the plant systems. Others may require a module or plant to shutdown. A major aim of this research is to define these fault conditions, propose methods for identifying the faults, and determine strategies for handling them.

- *Multi-module management*: A primary objective of supervisory control of SMRs is the ability to manage multiple SMR units from one control room. In this research, we aim to provide both increased supervision, monitoring, and coordination between plants. It must be realized that this objective must be balanced with operator oversight. The proper balance between operation and automation must be determined.

- *Load allocation*: This function is related to module management, salt vault operation, and economic dispatch. The proper power level for each reactor must be determined based upon future requirements for heat load for power generation and process heat. It should be realized that the salt vault provides the ability to generate electricity now for future needs. How these requirements are met by the various modules in order to operate safely and maximize plant efficiency is the focus of this function.

- *Mode transitions*: In the context of reactor operations, a mode is a particular regime of operation of the reactor and most generally includes power operations, start up, hot standby, hot shutdown, cold shutdown, and refueling. It should be obvious that a single plant that combines multiple SMR units, the various combination of modes can result in a large number of various modes for the plant. A broader definition of mode can include the various degraded states the plant may operate in due to faults and failures. The supervisory controller must be able to monitor in which mode each module operates and the fault state. In practice, the large number of possible combinations may be more than a human operator can manage, necessitating automated techniques.

- *Optimized plant performance*: This function is directly related to maximizing the economy of the plant. It may also consider other objectives for optimization, like personnel requirements, prognostics for component replacement, and various scheduling requirements.
- *Diagnostics and health monitoring*: Diagnostics and prognostics for health monitoring is a large area of research. In the context of this research, diagnostics is limited to fault diagnosis and the inference of plant or system health based upon an identified fault. For our purposes, a fault is the transition of a sub-system or component into a failed mode. The supervisory controller is appropriate for such diagnosis and health monitoring because it has access to data for an entire module or throughout the plant. Furthermore, the supervisory controller may have relaxed real-time requirements and can process large volumes of information throughout the history of the plant. More importantly, however, the ability to automate diagnostics and health monitoring can relieve the operator of some detailed chores that could otherwise interfere with the big-picture operation and management of the plant.

2.1.2 Architecture

Existing methods for control of nuclear plant processes are focused at the local level using decentralized, non-cooperative, fixed-gain designs. Local controllers lack coordination, and thus cannot achieve high, system-wide performance. The communication architecture describes which subsystems communicate which. The supervisory controller collects measurements from sensors and transmits data up the architecture. At various levels this data is processed by agents to produce useful information about the plant state and its health.

The approach that we have used is different from approaches that use a centralized controller that combine local control actions in a single multi-input/multi-output controller. While centralized control may have benefits, it is not feasible for SMRs since the design of the central controller must account for all reactors and their interaction with the BOP. The proposed approach provides capabilities that fit with SMR implementation including the use of multiple modules and multiple uses for generated heat.

The architecture has four levels:

1. *Operator level*: At the top level is the operator who oversees and manages the plant. Information presented to the operator must be relevant to the current mode of operation and the state of the plant. Commands are then transmitted down the architecture and combined with automated feedback control signals to direct the plant.
2. *Master level*: The top level is a central, supervisory coordinator that collects and transfers information from individual units, supervises their actions, and determines unit operating modes.
3. *Module (SMR) level*: Actions at this middle level monitor and control the SMR unit in order to meet operational requirements. The operating mode determined by the supervisory controller is used by the SMR unit to adjust its control parameters. The unit does this by adapting control processes as necessary.

4. *Local level*: The bottom level contains the local control loops for each unit (e.g., rod control, primary or secondary coolant flow control) whose purpose is to control the response of an individual unit. In principle, these loops are no different from existing controllers used in current I&C systems except that the architecture and the adaptive process proposed here allows for these controllers to be adjusted as needed.

Data is transmitted between these levels by four networks:

1. *Field bus*: The fieldbus uses an industrial computer network protocol for real-time distributed control. These protocols are standardized as IEC 61158. For the purposes of this research, the field bus transmits digital sensor signals to digital control systems (DCS) for real-time control at the local level. Importantly, these protocols used by the fieldbus are distinctly different from the other networks described below.

2. *Module network*: The module network transfers information between the local level and the module level. Sensor and controller signals are passed from a unit's local controllers to the module-level controller; these signals provide information about the modules's performance. The module-level controller can adjust local controllers to ensure the unit meets requirements of the operating mode specified by the supervisory controller.

3. *Plant network*: Signals used by the module-level controllers to optimize the modules's performance are sent to the plant level. These signals provide a combined picture of the total plant's condition. Based upon this and the dispatch requirements, the operating mode and power level of each SMR unit is specified.

4. *Operator network*: Information provided to the operators is transmitted to the control room via the operator network. Operator commands are then transmitted to the plant-level and other sub-level controllers.

2.2 Power Plant Simulation

In this research, we developed two simulations of advanced reactor designs: (i) SmAHTR, small modular advanced high temperature reactor; (ii) MSBR, molten-salt breeder reactor. The majority of the development in this work was for the SmAHTR design.

2.2.1 SmAHTR Reactor Simulation

During the course of this project, we were encouraged to focus our simulation and modeling attention on the SmAHTR (small modular advanced high-temperature reactor).[10] This model includes four SmAHTR reactors, three Brayton cycles, and a cooling tower in one integrated Simulink model. Since the intent of this research has been to create a fault-tolerant supervisory control system architecture, our objective has been to create a model that characterizes generally the plant dynamics and to limit the complexity of our approach to modeling the system; hence, the model describes time constants and transient response of system variable but is not necessarily a high-fidelity model of individual sub-systems. Where appropriate, assumptions about sub-system linearity or constant fluid properties were used.

Individual SmAHTR SMR modules as well as the SmAHTR plant have been programmed for real-time simulation in the Simulink Real-Time environment. Real-time simulation and experimentation enables for real-time controller parameter adjustments, disabling of reactor subsystems, adjustment of parameter values used in the model. Reference inputs for controllers can also be adjusted in real-time.

This capability is stressed in the context of the supervisory controller architecture definition, as the philosophical architecture that we have defined has been implemented on this platform. Automated decision making and "information compression" have been performed by the supervisory control system and are displayed, in real-time, on a graphical interface for interpretation and interaction with a human operator.

2.2.2 Molten Salt Breeder Reactor Simulation

Initially, the project was planned to develop supervisory control for a molten-salt breeder reactor. After discussions with the project manager, we changed our focus to a SmAHTR reactor. Work on the MSBR is summarized here.

The molten-salt breeder reactor (MSBR) is a single fluid 1000 MWe/2250 MWt, graphite-moderated reactor for steam-generated electricity production.[11] The reactor core is a 13 ft tall cylinder with two regions: a 14.4 ft wide central cylinder and a 1.25 ft thick outer annulus. The primary-loop fluid is a lithium fluoride-beryllium fluoride salt (FLiBe). The salt also contains a dissolved fuel mixture of ^{233}U and ^{232}Th, allowing it to act as both the fuel and coolant for the reactor. In addition to the reactor, the model includes four primary shell-and-tube heat exchangers, each employing four shell-and-tube super-critical steam generators[12]. Heat generated in the primary salt is transferred to a secondary salt in the primary heat exchangers. As noted, all four heat exchangers have four secondary loops that each feed four steam generators.

Circulating fuel reactor kinetics must account for the loss of delayed neutrons born outside the core[13]. To account for this loss, the model includes delay terms in the concentration equations. Due to hardware limitations, only four transport lag devices were available for the analog computer. The model includes a delay for the secondary salt transport to and from the primary heat exchanger and steam generator, leaving two devices for delays in the point kinetics. Thus, reactor neutronics were modeled by a two-group point kinetics equation. Physical constants for the model are given by Sides[12]. In the analog computer simulation, primary salt heat transfer coefficients were modeled by diode function generators; the relationships were provided in figure format only. For the real-time simulations, we fit a polynomial function for the heat transfer coefficient. The model includes a load control system designed to deliver steam at 1000 °F for nominal operation and to stay near that temperature during transients. The temperature of the steam is tightly coupled to the secondary salt flow rate, so the temperature controller adjusts secondary flow rate proportional to the error between the nominal steam temperature.

Testing was performed on the digital simulation and compared to the analog simulation results in Sides[12]. The digital and analog simulations agree, and the digital implementation of the control system responds in a similar fashion to the analog model. The simulated transients provoke the desired control responses, but the results do raise some questions. Some of the transients move the system beyond the realm of the physically feasible. There are also some refinements that can be made to improve the usefulness of result.

Chapter 3

Fault-tolerance of the supervisory control architecture

3.1 Fault-Tolerant Physical Systems

3.1.1 Fault Modeling

Sensor, Actuator, and Other System Faults

During normal operation of the reactor, we must anticipate faults in sensors and actuators. Ultimately, these faults manifest themselves in erroneous data being measured or incorrect control signals being applied. For the fault-tolerance approach we have taken in this research, we have been interested in specifically identifying the type of fault. This approach has the advantage that strategies specific to the particular fault can be implemented, and both monitoring and situational awareness are improved.

We have modeled various sensor, actuator, and other system faults in the SmAHTR system. These sensors and actuators have been chosen considering the functions of the supervisory control system; specifically, monitor the heat generation rate, monitor the heat removal rate, and govern heat flow.

- *Sensor Fault Models*: The sensor faults considered are (i) sensor noise (ii) sensor saturation (fails high or low) (iii) sensor drift (iv) loss of sensor These sensor faults have been applied to sensors identified previously in the SmAHTR plant simulation developed in this research.

- *Actuator Fault Models*: We have limited the actuator faults that we examined in this research to the secondary-side pump of the primary heat exchanger, and have considered a failure in only one loop. By design, the SmAHTR should be able to operate under normal conditions with only 2 of 3 primary heat exchangers operating. A fault in the pump results in zero flow in the loop and loss of heat removal capability.

- *Other System Fault Models*: We have considered a fault in the primary-loop RCP. We suppose that a motor failure occurs and that the pump coasts down to a zero mass flow rate. We model a change in the effective heat transfer coefficients (UA's) on the primary or secondary-side of the primary heat exchanger by suggesting that fouling or excessive tube plugging.

Decision Agent Faults

The supervisory controller is the combination of a number of decision agents that process data and information at each of the levels of control. As data is processed at each level, new information is gleaned from the data, and this information is used at higher levels in the supervisory controller to make decisions.

In contrast to sensor, actuator, and network faults, faults in decision agents can lead to errors in decision making and command action. In some sense, these errors are more insidious since the root cause might lie either in the processor itself or in the code that is running on it. It is well known that digital I&C is a topic of concern and importance in the nuclear industry. Proper consideration of the topic is a research project in itself, and the consideration of digital I&C within the context of supervisory control was beyond the scope of this project. Even so, we have attempted to outline generally some possible sources of faults in decision agents.

- *Hardware Faults*: Failure of processors will result in a failure of an agent, and the inability to process information.
- *Software Faults*: Software faults can be more insidious since they often are not recognized until an event occurs.
- *Supervisory Controller Faults*:
  - *Local Level Faults*: Such faults include failure of the local-level controller itself.
  - *Module Level Faults*: At the module level, the heat generation and flow to the balance of plant is monitored; also, fault detection and monitoring occurs. Failures in the agents themselves can lead to inaccurate estimates of heat generation or the omission of a fault.
  - *Master Level Faults*: The energy balance of the overall plant is monitored and controlled at the master level. Failure of these agents would result in inaccurate evaluation of this energy balance.
  - *Operator Faults*: The operator is the top-level decision agent. It should not be forgotten that human error is a prevalent source of faults, and can occur with higher frequency than for automated systems.

3.1.2 Fault-Tolerance Protocols

This section outlines the methods, or protocols, for handling faults. In general, the approach used in this research is to identify faults and apply appropriate remedies. This approach provides improved situational awareness since plant operation proceeds with the knowledge of a particular fault. This is in contrast to techniques, like voting or median select, that merely use redundancy to ensure fault-tolerance. More importantly, faulted systems can be replaced or repaired to return the plant to a state of nominal operation.[1] Thus, a benefit of this approach is improved online monitoring; thus, aspects of this meet objective III.

Handling Sensor, Actuator, and Other Faults

In this effort, faults are identified and then appropriate remedies are applied. Remedies for faults depend upon the component used. Redundant sensors provide multiple measurements and are appropriate for the techniques used.

[1] Nominal operation refers to the operating condition with all operating systems functioning normally. This is in contrast to normal operation, which refers to anticipated, regular operating conditions that do not require emergency or safety systems.

Handling Faults in Decision Agents

Faults in decision agents can be particularly troublesome since these agents process data and transmit information to other agents for decision making. The effect of decision agent faults on the performance of the supervisory controller is not a primary focus of this research. Even so, strategies can be implemented to minimize their effect. This section outlines some of the approaches that can be used for handling faults in decision agents.

- *Hardware Faults*: Diversity is the dominant paradigm for ensuring fault tolerance of digital I&C systems. Such diversity could be used to determine the presence of a fault. Diverse systems operating in parallel could be compared and anomalous results eliminated from consideration in decision making. The parallel approaches, both the hot-standby observers and parallel-filters, are attractive because the failure of a single agent in the parallel filter bank prohibits the use of a filter for a particular fault. Since other filters in the bank are still functional and fault-free, those faults and corresponding virtual sensors can still be used.

- *Software Faults*: Verification and validation (V&V) are the dominant paradigm for ensuring that software is fault free. Other verified models can be used as a reference for the purpose of V&V of supervisory control hardware. The use of standard algorithms and programs decreases the chance of faults in code. Such standard algorithms, like Kalman filtering algorithms, can be programmed once and verified to be bug-free. The use of such standard algorithms in different scenarios and architectures is possible due to the broad generality and application of such approaches.

3.2 Fault-Tolerant Network

The network in a nuclear power plant must be resilient. In this effort we have studied wireless networks as a backup network for supervisory control. We have defined fault models for the wireless network, and have defined the requisite fault-tolerant protocols for the network. These models will be implemented and integrated with our plant simulations for examining the performance of this cyber-physical system.

3.2.1 Network Topology

To gain more flexibility and efficiency in deploying relay nodes, we divide the network area into two regions: the k-connected region and the relay region. In the k-connected region, there are k edge-disjoint paths from the sensors to the virtual roots. The number of paths is set depending upon the current network link quality. The more edge-disjoint paths that are required, the more nodes that need to be active in the network, and the more robust the network is. In the relay region, there is a line of primary nodes and at most three lines of backup nodes from the virtual roots to the remote controller. Similarly, the more lines of backup nodes that are activated, the more reliable the network. We connect these two regions by virtual roots, special sensor nodes. Messages go from sensors to virtual roots, and then to the controller; the routing in each region is done differently. Note that all of the nodes in one level of the relay region can reach all of the nodes in the next level in our topology design.

3.2.2 Network Faults

Independent link and node failures can be instantiated by hardware failures. The hardware failure causes node or link (radio) failure with a certain fault probability with the fault and corresponding fault probability changing in time. In our model, a fault is a random Boolean variable, and at discrete time instants the fault occurs with some probability. It persists for a given time interval, called the fault duration. This results in a time-sequence of faults and fault probabilities. Our proposed fault duration concept applies to all the nodes/links in the network, even though each node/link has its own fault probability.

3.2.3 Handling Network Faults

We have designed the bitvector protocol. This uses broadcast and TDMA scheduling to guarantee real-time transmission, as follows: Relay nodes broadcast messages level by level towards the controller. Within each level, a primary node will broadcast first, then the first, second, and third backup nodes, in order. If the backup parent finds out, while overhearing and checking the bitvector, that the primary did not send out the values, then the backup parent compensates for that loss.

3.3 Networked Control Systems

Wireless control systems are composed of controllers, sensors, and actuators connected by a wireless network. Wireless control systems over multi-hop wireless sensor network have received significant attention in recent years.[14,15,16,17,18,19,20] Given that the control room is usually geographically distant from the sensors and actuators, wireless networks are good for place-and-play deployment due to the lack of wires (electrical or networking). However, wireless network delays to/from the control room and packet losses can induce serious errors in the control system, which is undesirable.

3.3.1 Network Configuration for Control

In this research, we have focused on multi-hop wireless network reconfiguration for control systems. We only consider link failures and define an average link success ratio (LSR) as the probability a message can be sent out successfully on that link. We use LSR as the indication of the average network interference.

We solve the problem in two parts, offline and online. For the offline part, in order to quantify the network imperfection, we propose a network imperfection model that transforms network delay and delivery ratio to the total induced delay on the control system. We estimate the total induced delay for a set of network configurations, including network topologies. We find an optimal estimated network configuration set for each LSR offline, and store them at the controller node. For the online part, at run time, the network notifies the controller what the estimated LSR is, and the controller selects a network configuration for the network from the ones computed offline. The controller then broadcasts the new network configuration to all the nodes in the network to carry out a reconfiguration. Therefore, the control node acts as a centralized network manager and decides which network configuration should be chosen.

There is a trade-off between network delay and packet losses for control system performance. Although the network-induced imperfection problem has been studied from the control system perspective,[21,22,23,24] minimizing the network-induced imperfections has not been studied from the network perspective. The trade-off between packet losses and delays can be achieved by controlling the network configuration. This problem can be thought of as an optimization to find the network configuration with minimum network imperfections; however, environments typically change with time and space.[25,26] Some interference can make nodes inaccessible and disconnected for a limited amount of time. This may severely impact the control system performance. Therefore, we propose online network reconfiguration to deliver the required control system performance.

3.3.2 Networked Control Performance

We have explored the effects network faults have on the closed-loop performance of the primary heat exchanger and pump system. We manipulate the input to the coolant pump dynamics remotely by sending the measurements through a wireless sensor network to the modular controller. In situations when the wireless sensor network is experiencing transmission error, we handle the transmission errors in several ways:

(i) A first approach used the last transmitted (received) packet in the controller until new measurements are received.

(ii) A second approach used an extended Kalman filter (EKF) to provide an estimate of the measurements and the primary heat exchanger dynamics, then the controller uses the estimated values.

(iii) A third approach uses model predictive control to calculate the control system for a particular network configuration.

We have demonstrated the performance of the wireless network on a single SmAHTR primary heat exchanger to produce a desired power demand level. The objective is to have the closed-loop primary heat exchanger power output track a reference power demand signal. The wireless network uses the bitvector protocol. The network reconfiguration algorithms are implemented on the modular-level controller, which updated the network configuration based on comparison with the offline network analysis.

We simulate our wireless network reconfiguration with the nonlinear primary heat exchanger system in a nuclear power plant. We combined the implementations of bitvector protocol with a state-of-the-art cyber-physical system simulator (WCPS 2.0[15]) and allow the wireless network to run together with the primary heat exchanger system Simulink model

There is a trade-off between the network performance and the control system performance. One approach to address the tradeoff is to use optimal control methods, in particular model predictive control (MPC) methods. MPC finds the future control signal that minimizes the mean squared error.[27] In this framework, the system model predicts its future response over a time-period, called the prediction horizon, and the future control signal is predicted over a different time-period, called the control horizon[27]. The MPC problem is solved at each time step to take into account current measurements. This allows for MPC to be combined with the wireless network because it can handle the measurable faults in its algorithm to minimize the cost function quantified the combined performance of the primary heat exchanger power tracking error and the wireless network. A second advantage to using MPC is the algorithm can handle constraints placed on the system's state and control. We demonstrated the closed-loop performance of the primary heat exchanger and pump dynamics when implementing the MPC. The demonstration is done using off-line analysis.

Chapter 4

Automated decision making and online monitoring

4.1 Machine Learning for Classification

We have used on supervised learning algorithms to classify sensor and actuator behavior. The machine learning classification problem is to classify signals using salient characteristics that best discriminate fault-free and faulted states. Data from fault-free and faulted components are mapped to these salient characteristics, and using these characteristics, fault-free and faulted are separated by a hyperplane. The objective of machine learning is to find the separating hyperplane so that the classification states can be most readily discriminated. One advantage of this approach is that many techniques from machine learning do not require one to explicitly model the dynamics of a particular process. Thus, such techniques are data-based rather than model-based. Additionally, many of the techniques used in machine learning have roots in probability theory, making many of these techniques well-suited for situations involving uncertainty.

Our classifier has been implemented in a real-time environment on an external computing machine for a model of a simplified point-kinetics model of an SMR. It was demonstrated that the regularized logistic regression is effective for fault identification and diagnosis. The statistical binary classification technique used is regularized logistic regression. Classifier training and optimization has been performed off-line, while the classifier itself functions in real-time. The simultaneous implementation of several class discriminating "fault observers" has been achieved in a real-time simulation environment for demonstrating classifier and technique performance.

The probabilistic nature of this approach makes it ideal for use with human operators, as the classifier can provide both operators and higher-level inference engines with a probabilistic estimate that a particular fault has occurred. Evidence of sensor faults can be aggregated in a database for evaluation by a higher-level probabilistic inference engine, such as a Bayesian network, for determining the onset of equipment or sensor degradation.

Current on-line monitoring techniques used in the nuclear industry do not explicitly classify specific sensor anomalies, which could be used as prognostic indicators of sensor or equipment degradation. Class-discriminative models can be used to identify specific faults by training a model to recognize the characteristics that are features of the faults. The probabilistic nature of this approach makes it appropriate for use with human operators, as the classifier provides a high-level inference engine that yields an estimate of a particular fault and a corresponding conditional probability that provides a measure of belief in the estimate itself. It should be acknowledged that this belief is not the same as uncertainty. Rather, the probability produced is a measure of the degree of belief in a particular classification. Evidence of sensor faults can be aggregated in a database for further evaluation by a higher-level engine, such as a Bayesian network, to determine the equipment or sensor degradation. Using a supervised learning algorithm such as logistic regression in concert with the a parity relationship, Mutlivariate State Estimation Technique (MSET), or ANMP could serve as an effective tool for SMR plant operation.

4.2 Hot-Standby State Observers

State observers can be used when a sensor reading becomes suspect. Provided that a condition on observability is met, suspect measurements may be ignored and replaced by the output of a state observer. The state observer provides an estimate of the true state by recursively using the inputs and outputs from the actual dynamic system. By design, the estimated state quickly converges to the true state. A bank of state observers representing every combination of observable, faulted system, can be designed and then operated continuously: in this sense, the state observers are in a hot-standby mode. Once a fault is detected, the estimated state corresponding to the measurement that is now faulted is brought live. A hot swap is performed by ignoring a suspect measurement and relying on the state observer estimate.

Initialization of a hot standby state observer can be triggered when the belief in a particular fault is greater than some threshold. An estimation of the state affected by this faulty behavior will be augmented with the remaining, healthy sensor readings for the automatic and operator-driven decisions. The operator can be notified that a state estimate is being used so that subsequent decisions may be made about the disposition of the now-faulted sensor.

We evaluated all possible degraded measurements of statistical significance for the salt vault subsystem. For observable cases, state observers were designed. To determine when a fault occurred, we used logistic regression. A sensor fault was introduced at an arbitrarily-selected point in simulation time. Positive identification of the fault occurs when the degree of belief exceeds some threshold. When this occurs we update the output matrix of the salt vault model, thus ignoring the faulted state measurement. Measurements with faults are replaced by corresponding signals from the hot standby state observer.

4.3 Parallel-Filter Techniques

Two things are of interest for fault identification and fault-tolerance in a supervisory control system.

1. How to determine if a particular fault has occurred;
2. How to determine the state of the system when the signal model is unknown (because of a fault).

The field of system and control theory that is interested in these questions is adaptive estimation, and there are well established methods and algorithms for achieving both tasks. Different approaches can be applied to the adaptive estimation problem, including parallel processing techniques[28,29,30] and sequential Monte Carlo techniques.[31] In this research, we have developed how parallel processing techniques can be used to determine the state and fault-condition of the system. Parallel processing techniques are attractive because they can be implemented using parallel computing architectures, which are now well established, inexpensive, and easy to construct and expand.

The approach is as follows: the unknown parameter is discrete has a finite number of points, and each point has a known or assumed a priori probability. The estimator includes a parallel bank of N state estimators. These estimators can be a kind that is appropriate to the problem: Kalman filters for linear stochastic systems, extended Kalman filters and Unscented Kalman filters for non-linear systems with near Gaussian statistics, and particle filters for general non-linear/non-Gaussian systems.[31,32,33] The chosen estimator is driven by noisy signal measurements, with the ith estimator designed on the assumption the unknown parameter is correct for this estimator.

The probability that a particular value of the unknown parameter is correct is updated recursively using with Bayes' rule. Bayes' rule transforms a priori (pre-measurement) probabilities to a posteriori (post-measurement) probabilities. The specific problem then is determining the likelihood function of the measurement given a particular value of the unknown parameter. Various filtering methods can be used to calculate this likelihood function. The Kalman filter[28] and its enhancements and extensions, the extended Kalman filter,[28] and unscented Kalman filter[34] among others are easily formulated to do this. Each of these approaches can be setup using parallel processing techniques making the implementation of real-time PRA possible. For systems that are non-linear/non-Gaussian, sequential Monte Carlo techniques like particle filters[32] can be used. These techniques can also be parallelized enabling real-time processing.

Chapter 5

Bibliography

[1] G. D. Storrick, B. Petrovic, and L. Oriani. Supervisory control strategy development. Final Report STD-AT-07-01 (rev. 1), Westinghouse Electric Company, LLC, 2007.

[2] G.D. Storrick and M.D. Carelli. The IRIS (International Reactor Innovative and Secure) and its unique advancement of the state-of the art. In *IEEE Power and Energy Society 2008 General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*, 2008.

[3] D. Clayton and R. Wood. The role of instrumentation and control technology in enabling deployment of small modular reactors. In *ANS NPIC & HMIT*, 2010.

[4] H. Basher and J. S. Neal. Autonomous control fo nuclear power plants. Technical Report ORLNL/TM-2003/252, Oak Ridge National Laboratory, 2003.

[5] B.R. Upadhyaya, S.R.P. Perillo, X. Xu, and F. Li. Advanced control design, optimal sensor placement, and technology demonstration for small and medium nuclear power reactors. In *International Conference on Nuclear Engineering, Proceedings, ICONE*, volume 5, pages 763 – 773, 2009.

[6] S. R. P. Perillo, B. R. Upadhyaya, and F. Li. Control and instrumentation strategies for multi-modular integral nuclear reactor systems. *IEEE Trans. on Nuclear Science*, 58(5):2442–2451, 2011.

[7] A. J. Wood and B. F. Wollenberg. *Power Generation, Operation, and Control*. John Wiley & Sons, Inc., 1996.

[8] D. G. Cole. Adaptive identification and control for small modular reactors. In *Proc. ASME 2011 Small Modular Reactor Symposium*, ASME 2011 Small Modular Reactor Symposium, 2011.

[9] S.M. Cetiner, D.L. Fugate, R.A. Kisner, and R.T. Wood. Functional requirements for supervisory control of advanced small modular reactors. Technical Report SMR/ICHMI/ORNL/TR-2013/03, Oak Ridge National Laboratory, 2012.

[10] S. R. Greene et al. Pre-conceptual design of a flouride-salt-cooled small modular advanced high-temperature reactor (SmAHTR). Technical Report ORNL/TM-2010/199, Oak Ridge National Laboratory, 2010.

[11] Roy C Robertson. Conceptual design study of a single-fluid molten-salt breeder reactor. Technical report, Oak Ridge National Lab., Tenn.(USA), 1971.

[12] W. H. Sides. MSBR control studies: Analog simulation program. Technical report, Oak Ridge National Laboratory, 1971.

[13] John MacPhee. The kinetics of circulating fuel reactors. *Nuclear Science*, 1958.

[14] S. Han, X. Zhu, A. Mok, D. Chen, and M. Nixon. Reliable and real-time communication in industrial wireless mesh networks. In *17th IEEE Real-Time and Embedded Technology and Applications Symp*, 2011.

[15] Bo Li, Lanshun Nie, Chengjie Wu, Humberto Gonzalez, and Chenyang Lu. Incorporating emergency alarms in reliable wireless process control. In *Int'l Conference on Cyber-Physical Systems*, pages 218–227. ACM, 2015.

[16] Bo Li, Yehan Ma, Tyler Westenbroek, Chengjie Wu, Humberto Gonzalez, and Chenyang Lu. Wireless routing and control: a cyber-physical case study. In *ACM/IEEE International Conference on Cyber-Physical Systems*, 2016.

[17] Miroslav Pajic, Shreyas Sundaram, George J Pappas, and Rahul Mangharam. The wireless control network: A new approach for control over networks. *IEEE Transactions on Automatic Control*, 56(10):2305–2318, 2011.

[18] Miroslav Pajic, Shreyas Sundaram, George J Pappas, and Rahul Mangharam. Topological conditions for wireless control networks. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pages 2353–2360. IEEE, 2011.

[19] Wenchen Wang, Christopher D'Angelo, Daniel Mosse, and Daniel Cole. Integrating control and fault-tolerant wireless network design for small modular nuclear reactors. In *Information Reuse and Integration (IRI), 2016 IEEE 17th International Conference on*, pages 332–342, 2016.

[20] Kyoung-Dae Kim and PR Kumar. The importance, design and implementation of a middleware for networked control systems. In *Networked Control Systems*, pages 1–29. Springer, 2010.

[21] Hongbo Li, Mo-Yuen Chow, and Zengqi Sun. Optimal stabilizing gain selection for networked control systems with time delays and packet losses. *IEEE Transactions on Control Systems Technology*, 17(5):1154–1162, 2009.

[22] Ahmet Onat, Teoman Naskali, Emrah Parlakay, and Ozan Mutluer. Control over imperfect networks: Model-based predictive networked control systems. *IEEE Transactions on Industrial Electronics*, 58(3):905–913, 2011.

[23] Gilberto Pin and Thomas Parisini. Networked predictive control of uncertain constrained nonlinear systems: recursive feasibility and input-to-state stability analysis. *IEEE Transactions on Automatic Control*, 56(1):72–87, 2011.

[24] Alphan Ulusoy, Ozgur Gurbuz, and Ahmet Onat. Wireless model-based predictive networked control system over cooperative wireless network. *IEEE Transactions on Industrial Informatics*, 7(1):41–51, 2011.

[25] Nouha Baccour, Anis Koubâa, Luca Mottola, Marco Antonio Zúñiga, Habib Youssef, Carlo Alberto Boano, and Mário Alves. Radio link quality estimation in wireless sensor networks: a survey. *ACM Trans on Sensor Networks*, 8(4):34, 2012.

[26] Vehbi C Gungor, Bin Lu, and Gerhard P Hancke. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE transactions on industrial electronics*, 57(10):3557–3564, 2010.

[27] Liuping Wang. *Model predictive control system design and implementation using MATLAB®*. Springer Science & Business Media, 2009.

[28] B. D. O. Anderson and J. B. Moore. *Optimal Filtering*. Prentice-Hall, 1979.

[29] D. G. Lainiotis. Optimal adaptive estimation: Structure and parameter adaption. *IEEE Trans. Autom. Contr.*, 16(2):160–170, 1971.

[30] P. K. S. Tam and J. B. Moore. Adaptive estimation using parallel processing techniques. *Computers & Electrical Engineering*, 2(2-3):203–214, 1975.

[31] O. Cappe, S. J. Godsill, and E. Moulines. An overview of existing methods and recent advances in sequential monte carlo. *Proc. of the IEEE*, 95(5):899–924, 2007.

[32] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp. A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking. *IEEE Trans. Sig. Proc.*, 50(2):174–188, 2002.

[33] O. Brun, V. Teuliere, and J.-M. Garcia. Parallel particle filtering. *Journal of Parallel and Distributed Computing*, 62(7):1186–1202, 2002.

[34] S. Julier and J. Uhlmann. Unscented filtering and non linear estimation. *Proc. of the IEEE*, 92(3):401–422, 2004.

Chapter 6

Publications and Presentations

6.1 Publications

- W. Wang, C.J.D'Angelo, D.Mosse, D.G.Cole. Integrating Control and Fault-Tolerant Wireless Network Design for Small Modular Nuclear Reactors, *IEEE 17th Conference on Information Reuse and Integration.* Pittsburgh, PA, pp. 332–342, July 28–30, 2016.

- W. Wang, D.Mosse, D.G. Cole. Bitvector: Fault Tolerant Aggregation Scheme for Monitoring in Nuclear Power Plants, *IEEE 12th International Conference on Embedded Software and Systems (ICESS)*, New York, NY, pp. 1166–1174, Aug 24–26, 2015.

- C.J.D'Angelo, C.J.Hansen, D.G. Cole, Using Pattern Recognition for On-line Sensor Prognostics and Diagnostics in Nuclear Power Plants, *9th International Conference on Nuclear Plant Instrumentation, Control, & Human-Machine Interface Technologies*, Charlotte, NC, pp. 1420–1429, February 23–26, 2015.

- C.J.D'Angelo, D.G. Cole. Hot Standby State Observers for Sensor Fault Tolerance in Small Modular Nuclear Reactors, *2015 American Nuclear Society Winter Meeting and Technology Expo*, Washington D.C., pp. 182–185, November 8–12, 2015.

- J.A. Farber, D.G. Cole. Real-Time Supervisory Control Implementation of SmAHTR Power Plant, *10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*, San Francisco, CA, pp. 322–330, June 11–15, 2017.

- J.G. Pickel, D.G. Cole. Real-Time Fault Detection and Transient Identification Using Extended Kalman Filters, *10th International Topical Meeting on Nuclear Plant Instrumentation*, Control and Human Machine Interface Technologies, San Francisco, CA, pp. 1133–1141, June 11–15, 2017.

6.2 Presentations

- J.A. Farber, D.G. Cole. Real-Time Supervisory Control Implementation of SmAHTR Power Plant, *10th International Topical Meeting on Nuclear Plant Instrumentation*, Control and Human Machine Interface Technologies, San Francisco, June 11–15, 2017.

- J.G. Pickel, D.G. Cole. Real-Time Fault Detection and Transient Identification Using Extended Kalman Filters, *10th International Topical Meeting on Nuclear Plant Instrumentation*, Control and Human Machine Interface Technologies, San Francisco, June 11–15, 2017.

- W. Wang, D.Moss, D.Cole, J.Pickel. Wireless Network Reconfiguration for Control Systems, *Real-Time and Embedded Technology and Application Symposium (RTAS)*, Pittsburgh, USA, April 18–21, 2017.
- C.J.D'Angelo, D.G. Cole. Real-Time Simulation and Control of Coupled SmAHTR Reactors, *2016 American Nuclear Society Winter Meeting and Technology Expo*, Las Vegas, NV, 2016.
- C.J.D'Angelo, C.J.Hansen, D.G. Cole. Using Pattern Recognition for On-line Sensor Prognostics and Diagnostics in Nuclear Power Plants, *9th International Conference on Nuclear Plant Instrumentation, Control, & Human-Machine Interface Technologies*, Charlotte, NC, 2015.
- C.J.D'Angelo, D.G. Cole. Hot Standby State Observers for Sensor Fault Tolerance in Small Modular Nuclear Reactors, *2015 American Nuclear Society Winter Meeting and Technology Expo*, Washington, D.C., 2015.
- W. Wang, D.Moss, D.Cole, J.Pickel. Cross-layer Real-time Scheduling for Wireless Control System, *Real-Time and Embedded Technology and Application Symposium (RTAS)*, Pittsburgh, April 18–21, 2017.

Appendix A

Quad Chart

U.S. DEPARTMENT OF ENERGY

Nuclear Energy

Advanced I&C for Fault-Tolerant Supervisory Control of Small Modular Reactors

OVERVIEW

Purpose: The purpose of this research is to develop supervisory control of small modular reactors (SMRs). We will also investigate techniques for fault-tolerance to maintain operational normalcy in the presence of anomalies. Online monitoring will be used to track system transients, thus avoiding undesirable reactor trips and diversion events.

Objectives:

- Develop an interconnected, hierarchical, supervisory control architecture. The supervisory controller would have several functions which may include module management, load allocation, manage plant performance, and monitoring.
- Fault-tolerance of the supervisory control architecture: Fault tolerance will be included as needed at the various levels of supervisory control. This redundancy is needed due to the variety of failures that can occur in such networks, particularly in a nuclear environment. We will study both node and link failures, for both correlated and independent faults.
- Online monitoring for decision making: We will develop methods to monitoring system signals, but comparing them against models of the system used by the supervisory controller.

IMPACT

Logical Path: The effort of this project comes in three work areas that follow the objectives:

- Supervisory control: this will define the details of the supervisory controller, incorporate that into a simulation, and perform appropriate testing of the controller.
- Fault tolerance: This will define fault models of the simulated SMR plant and supervisory controller. Real-time, fault-tolerant protocols will be defined and implemented in simulations.
- Online monitoring: Operating modes and normal/abnormal transients for SMRs will be identified. Tools for monitoring these operating modes, plant transients, and faults will be implemented in simulations and evaluated.

Outcomes: The proposed outcomes of this project are as follows:

- A system architecture for a supervisory I&C control system for an appropriate SMR plant system.
- SMR online monitoring methods and procedures.
- Fault-tolerant techniques, procedures, and protocols.
- Simulations of the supervisory system for suitable normal and abnormal transient events.

DETAILS

Principal Investigator: Daniel G. Cole

Institution: University of Pittsburgh

Collaborators: Daniel Mossé, Computer Science, University of Pittsburgh

Duration: 3 years **Total Funding Level:** $800,000

TPOC: Sacit Cetiner

Federal Manager: Brian Robinson

Workscope: RC-2.1

PICSNE Workpackage #:
NU-13-PA-PITT-0301-03

RESULTS

Results:

We have the following accomplishments:

- Development of a supervisory control system
- Development of real-time simulations of MSBR and SmAHTR designs
- Simulation of the supervisory control system in Matlab/Simulink and on real-time platforms
- Fault-tolerance of physical system failures
- Fault-tolerance of network systems
- An analysis of networked control systems that accounts for the impact if network delays and errors on the control system's performance
- The use of machine learning for fault-detection and diagnosis
- Development of hot-standby observers to monitor the plant in the event of sensor failures
- Use of parallel processing techniques for adaptive estimation of plant faults; this enables the detection of faults.