OAK RIDGE
NATIONAL LABORATORY
MANAGED BY UT-BATTELLE
FOR THE DEPARTMENT OF ENERGY

ORNL/TM-2013/320
SMR/ICHMI/ORNL/TR-2013/04

Definition of Architectural Structure for Supervisory Control System of Advanced Small Modular Reactors

August 2013

Prepared by

Sacit M. Cetiner
Daniel G. Cole
David L. Fugate
Roger A. Kisner
Michael A. Kristufek
Alexander M. Melin
Michael D. Muhlheim
Nageswara S. Rao
Richard T. Wood

UT-BATTELLE
ORNL-27 (4-00)

ORNL/TM-2013/320
SMR/ICHMI/ORNL/TR-2013/04

Reactor and Nuclear Systems Division

DEFINITION OF ARCHITECTURAL STRUCTURE FOR SUPERVISORY CONTROL SYSTEM OF ADVANCED SMALL MODULAR REACTORS

Sacit M. Cetiner (Principal Investigator)
Daniel G. Cole (University of Pittsburgh)
David L. Fugate
Roger A. Kisner
Michael A. Kristufek (University of Pittsburgh)
Alexander M. Melin
Michael D. Muhlheim
Nageswara S. Rao
Richard T. Wood (Project Manager)

This report fulfills the milestone M3SR-13OR1301072,
"*Establish Functional Architecture for Supervisory Control of Advanced SMR Plant*".

Date Published: August 2013

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ADS	Automatic Depressurized System
AFSM	Augmented Finite State Machine
ALMR	Advanced Liquid Metal Reactor
AdvSMR	Advanced Small Modular Reactor
BLC	Block Level Controller
BOP	Balance of Plant
CAPV	Control Action Prediction and Validation Module
CGM	Command Generation Module
CIP	Critical Infrastructure Protection
CONOPS	Concept of Operations
COTS	Commercial Off the Shelf
DAP	Diagnostics and Prognostics Module
DAQ	Data Acquisition Module
DBE	Design Basis Event
DCS	Distributed Control System
DDS	Data Display and Processing System
DOE	US Department of Energy
EM	Electromagnetic
ERM	Enhanced Risk Monitors
ESFAS	Engineered Safety Features Actuation System
FDI	Fault Detection and Isolation
FMEDA	Failure Modes, Effects, and Diagnostics Analysis
HMI	Human Machine Interface
ICHMI	Instrumentation, Control and Human-Machine Interface
ICI	Instrumentation and Controls Infrastructure
ICS	Instrumentation and Control System
IHTS	Intermediate Heat Transport System
IHX	Intermediate Heat Exchanger
IM	Integrated Master
IT	Information Technology
LWR	Light Water Reactor
MBSE	Model-Based System Engineering
MIMO	Multiple-Input Multiple-Output
MLD	Master Logic Diagram
MMI	Man Machine Interfaces
MPC	Model Predictive Control
NE	Office of Nuclear Energy
NERC	North American Electric Reliability Corporation
NSSS	Nuclear Steam Supply System
O&M	Operations and Maintenance
OCS	Operation and Control Centers System
P	Proportional
PAS	Planning and Scheduling Module
PB	Power Block
PCS	Plant Control System
PCS	Power Conversion System
PDSS	Post-Deployment Software Support
PFD	Probability of Failure on Demand

PHTS	Primary Heat Transport System
PI	Proportional-Integral
PID	Proportional-Integral-Derivative
PLC	Plant Level Controller
PNNL	Pacific Northwest National Laboratory
PRISM	Power Reactor Inherently Safe Module
PSA	Plant Status Analysis Module
PSAM	Plant Status Analysis Module
PSM	Planning and Scheduling Module
RC	Reactor Controller
RM	Reactor Module
RO	Reactor Operator
RPS	Reactor Protection System
RTS	Reactor Trip System
RUL	Remaining Useful Life
SC	Signal Conditioner
SCS	Supervisory Control System
SIL	Safety Integrity Level
SISO	Single-Input Single-Output
SMR	Small Modular Reactor
SPA	Sense-Plan-Act
SPE	Sense-Plan-Execute
SSC	Structures, Systems, and Components
SysML	Systems Modeling Language
UHS	Ultimate Heat Sink
ULD	Unit Load Demand
UML	Unified Modeling Language

EXECUTIVE SUMMARY

Small modular reactors (SMRs) can provide the United States with a safe, sustainable, and carbon-neutral energy source. Because of their small size and, in many cases, simplified nuclear island configurations, it is expected that capital costs will be significantly less for SMRs compared to that of large, Generation III+ light-water reactors. Advanced SMRs, which use coolants other than water as the primary heat transport medium, can enhance the simplicity gains by introducing several passive safety and control characteristics.

The benefits of SMRs can include reduced financial risk, operational flexibility, and modular construction. Achieving these benefits can lead to a new paradigm for plant design, construction and management to provide for multi-unit, multi-product-stream generating stations while addressing the need to compensate for reduced economy-of-scale savings. However, there are technology needs that must be addressed to resolve challenges to establishing this new paradigm. This condition is particularly true for the unique characteristics and harsh environments associated with advanced SMR concepts. Consequently, the U.S. Department of Energy (DOE) Office of Nuclear Energy (NE) established the Advanced SMR (AdvSMR) Research and Development (R&D) Program.

The economic factor most strongly affected by the loss of economy of scale is the day-to-day cost of plant management. The controllable day-to-day costs of SMRs are expected to be dominated by operation and maintenance (O&M) costs, which are heavily dependent on staffing size and plant availability. Efficient, effective operational approaches and strategic maintenance can help contain these costs and ensure economic viability.

Instrumentation, control, and human-machine interface (ICHMI) technologies provide the foundation for what is the equivalent of the central nervous system of a nuclear power plant. Therefore, innovative use of intelligent automation can have a significant impact on optimizing plant staffing and controlling O&M costs. Essentially, the economy of automation can serve as a compensating factor for the loss of economy of scale.

Unfortunately, highly automated, intelligent control capabilities have not been demonstrated for nuclear power plant operations and there is limited experience in other application domains. Supervisory control provides a means for the integration of control, decision, and diagnostics to support extensive automation. The targets for automation include operational management of highly complex plants, dynamic management and control of multiple product streams from a plant, and coordinated management of multiple modules.

Within the ICHMI technical research area under the AdvSMR R&D program, the Supervisory Control of Multi-Modular SMR Plants project was established to proceed with development and demonstration of the architectural framework and foundational modules that are needed to facilitate the integration of control, decision, and diagnostics to support the necessary level of automation.

This technical report documents the findings from the second phase of research activities for the Supervisory Control project. Specifically, the report defines and documents strategies, functional elements, and architectural structure for supervisory control of an advanced SMR plant. This current research builds on the previous phase that provided important background information: (1) document the state-of-the-practice based on an investigation of research and applied experience with supervisory control concepts in both nuclear and non-nuclear applications and (2) develop high-level functional requirements for anticipated operational scenarios for multi-modular plants as well as knowledge of prior control approaches for complex systems to define necessary supervisory control capabilities.

More specifically, this report advances the state-of-the art by incorporating decision making into the supervisory control system architectural layers through the introduction of a tiered-plant system approach. The findings documented in this report provide the basis for the next phase of the project wherein foundational modules will be developed and demonstrated for achieving supervisory control to implement command decisions based on plant status, component condition, and process data. The next phase will enable the theory of supervisory control to be applied through simulation of a representative multi-unit AdvSMR plant concept.

The research findings are captured in this report through provision of a brief history of hierarchical functional architectures and the current state-of-the-art description of a reference AdvSMR to show the dependencies between systems, presentation of a hierarchical structure for supervisory control, description of the importance of understanding trip setpoints, application of a new theoretic approach for comparing architectures, identification of cyber security controls that should be addressed early in system design, and description of ongoing work to develop system requirements and hardware/software configurations.

The concepts of systems functionality, performance and stability, environment, communications, reliability, testability, maintainability, human-machine interface, and security were investigated in the context of supervisory control. Modern control systems for mission-critical industries such as aerospace, nuclear, chemical, and defense require multidisciplinary system engineering during all phases of the project. However, the software engineering skills to create robust functional architectures to support high degrees of automation are not commonplace. Architectures, in general, have distinct features that lead to different properties, which then lead to support specific capabilities. The choice of features is often made by following explicit methodological assumptions, driven by the domains and environments for which the design will be implemented.

Early highly automated or autonomous architectures adopted a basic structure designated as *sense-plan-act* (SPA) or *sense-plan-execute* (SPE). In the mid-1980's, a layered architecture identified as the *subsumption architecture* was developed for autonomous robots. Numerous robotic and space applications have adopted and expanded the concept. The basic three-layer architecture organizes control algorithms in terms of the functional layer (also called *controller* layer), the coordination layer (also called *sequencer* layer), and the organization layer (also called *deliberator* layer). The layered structure results in successive delegation of duties from higher levels to lower levels; hence, the number of distinct tasks increases as one goes down the hierarchy. Higher levels are concerned with slower aspects of system's behavior while responsible for planning with a longer time horizon while the lower levels accomplish real-time action to address the immediate conditions. Based on experience with autonomous applications for robotic and space application, it is clear that a three-layer architecture provides an appropriate basis for the supervisory control system architecture being developed in this research.

This research uses the advanced liquid-metal reactor (ALMR), which is modeled after the General Electric Company PRISM reactor as documented in the early 1990s, as the baseline advanced SMR design both for the current study and for future modeling and simulation. The ALMR PRISM design utilizes nine reactor modules arranged in block of three. One turbine-generator is assigned to each power block. A steam generator is assigned to each reactor. The ALMR PRISM small modular reactor design had previously undergone a level of design that is documented in design reports so adequate information is available. Given its approach to modularity and extensive coupling among units, the ALMR PRISM serves as a suitable reference concept.

The present research defines a structure and architecture of a supervisory control system for advanced SMRs that has the features of planning and scheduling, analyzing plant status, diagnosing problems as they develop and predicting potential future problems, making decisions based on these features, and

generating validated commands to lower structures in the plant. For control purposes, the plant is divided into three tiers, corresponding to a system's relationship to the main flow of energy through the plant—that is, from the reactor to the generator and the ultimate heat sink.

A system-level functional taxonomy was established to define interface relationships between the supervisory control system and plant systems. Tier-I systems involve the direct pathway of transporting heat from the source to the sink. Tier-II systems provide direct support to Tier-I systems. Tier-III systems are the common utilities and services that supply bulk materials to the Tier-I and Tier-II systems. The supervisory control concepts and architectures developed in this research apply to the Tier-I and Tier-II systems.

The functions of the supervisory control system are designed to require minimal human intervention in both normal and abnormal operations. One of the chief functions of the supervisory control systems is to prevent excursion into the trip regime of the reactor protection system. This function is accomplished by vigilant monitoring of equipment status, measured parameters, predicted outcomes, and internal states to make decisions that generate appropriate set points, valve alignments, and other configuration structures.

Concepts of metrics of effectiveness for supervisory control were investigated. Because information is the principal part of the decision-making process, information entropy can be used as a measure of the uncertainty in that information and hence the decision-making process. Information entropy was investigated as a method to compare control architectures. An automatic depressurization system was used a test example to compare a probabilistic risk-based assessment against an entropy-based assessment. The entropy-based method correlated well in the limited test. The entropy-based method has application in evaluating disparate architectures. In addition, this method has potential for on-line, real-time estimation of system uncertainty in the decision-making process.

The cyber infrastructure for a SMR requires a combination of defenses that protects both I&C networks and information (e.g., plant or corporate) networks. Current capabilities are combinations of network security, cyber-resilient controllers, and anomaly detection. The cyber security challenge for the I&C network for an advanced SMR extends beyond the usual best cyber security practices. It requires implementation of strict configuration management and control practices of not only hardware and software components but also planning and execution of proper concepts of operations (CONOPS) that define physical and network access rights and software and hardware maintenance and upgrades—including supply chain management. Ongoing research to develop inherent resilience in real-time feedback controllers will result in mathematical techniques to successfully detect and continue system operation after a successful cyber penetration.

ABSTRACT

This technical report was generated as a product of the Supervisory Control for Multi-Modular SMR Plants project within the Instrumentation, Control and Human-Machine Interface technology area under the Advanced Small Modular Reactor (SMR) Research and Development Program of the U.S. Department of Energy. The report documents the definition of strategies, functional elements, and the structural architecture of a supervisory control system for multi-modular advanced SMR (AdvSMR) plants. This research activity advances the state-of-the art by incorporating decision making into the supervisory control system architectural layers through the introduction of a tiered-plant system approach. The report provides a brief history of hierarchical functional architectures and the current state-of-the-art, describes a reference AdvSMR to show the dependencies between systems, presents a hierarchical structure for supervisory control, indicates the importance of understanding trip setpoints, applies a new theoretic approach for comparing architectures, identifies cyber security controls that should be addressed early in system design, and describes ongoing work to develop system requirements and hardware/software configurations.

1. INTRODUCTION

The U.S. Department of Energy (DOE) Office of Nuclear Energy (NE) established the Instrumentation, Control and Human-Machine Interface (ICHMI) technology area under the Advanced Small Modular Reactor (SMR) Research and Development (R&D) Program to contribute to the resolution of significant technical hurdles to design completion and commercialization of advanced SMRs (AdvSMRs).[*] These technical challenges arise from the unique features and characteristics inherent to their compact designs. As part of the AdvSMR R&D program, the Supervisory Control of Multi-Modular SMR Plants project was established to enable innovative control strategies and methods to supervise multi-unit plants, accommodate shared systems, identify opportunities to increase the level of automation, define economic metrics based on the relationship between control and staffing levels, and permit flexible co-generation operational regimes.

This technical report documents the findings from the second phase of research activities for the Supervisory Control project. Specifically, the report defines and documents strategies, functional elements, and architectural structure for supervisory control of an advanced SMR plant. This current research builds on the previous phase that provided important background information: (1) document state-of-the-practice based on an investigation of research and applied experience with supervisory control concepts in both nuclear and non-nuclear applications and (2) develop high-level functional requirements for anticipated operational scenarios for multi-modular plants as well as knowledge of prior control approaches for complex systems to define necessary supervisory control capabilities.

More specifically, this report advances the state-of-the art by incorporating decision making into the supervisory control system architectural layers[†] through the introduction of a tiered-plant system[‡] approach. The findings documented in this report provide the basis for the next phase of the project wherein foundational modules will be developed and demonstrated for achieving supervisory control to implement command decisions based on plant status, component condition, and process data. The next phase will enable the theory of supervisory control to be applied through simulation of a representative multi-unit AdvSMR plant concept.

To better understand the architecture for the proposed supervisory control system, this report

- provides a brief history of hierarchical architectures and the current state-of-the-art,
- describes a reference AdvSMR to show the dependencies between systems,
- presents the hierarchical structure of an advanced supervisory control system based on a tiered organization of plant systems,

[*] An advanced reactor is defined as a nuclear reactor that uses coolant other than water as the primary heat transport medium. Hence, AdvSMRs are small modular reactors with non-water coolant in the primary loop.

[†] The supervisory control system architectural layers, which are described in Section 4.4, are
- Organizational layer,
- Coordination layer, and
- Functional layer.

[‡] The tiered-plant system approach, which is described in Section 4.7, divides the systems into the following tiers:
- Tier I—systems directly involved in heat transport,
- Tier II—support systems, and
- Tier III—utility systems.

- describes the importance of understanding trip setpoints,
- applies a new theoretic approach for comparing architectures,
- identifies cyber security controls that should be addressed at the beginning, and
- describes ongoing work to develop system requirements and hardware/software configurations.

1.1 OPERATIONAL FLEXIBILITY OF ADVANCED SMRS

The benefits of AdvSMRs can include reduced financial risk, operational flexibility, and modular construction. Achieving these benefits can lead to a new paradigm for plant design, construction and management to provide for multi-unit, multi-product-stream generating stations while addressing the need to compensate for reduced economy-of-scale savings.

Advanced SMRs can provide operational flexibility to address considerations such as grid stability and generation of alternate or multiple products (e.g., electricity, process heat, hydrogen, and freshwater). This concept is described as a nuclear hybrid energy system [1]. The first consideration introduces unique operational scenarios and values flexibility. Automated load following for AdvSMRs can offset the grid impact of intermittent power generators such as wind turbines or photovoltaic arrays. Additionally, an AdvSMR may be responsible for responding to grid upsets rather than isolating itself from the grid. For example, the AdvSMR may be required to support a "black" startup to bootstrap the power grid into operation. The second consideration may introduce unique plant management scenarios and control regimes associated with automatic reconfiguration of the balance of plant to dynamically transition among product streams or arising from dynamic coupling among units due to shared or transitioning systems.

Flexible plant management through new operational concepts to support a variety of product demand scenarios can facilitate highly efficient, effective use of multiple small units [1]. Advanced SMR designs can provide the benefit of sustained output from a plant composed of multiple modules. By building a large power park of many AdvSMR modules, the plant provides the advantage of only losing a small percentage of its power output should one unit be out of service for a planned outage or unplanned trip. Additionally, the provision of multiple product streams enables effective utilization of the energy content of the heat generated by the reactor. Essentially, the plant can be reconfigured to meet demand. For example, electrical power could be the exclusive product during high-demand periods and some units could be switched to hydrogen production during overnight, low-demand periods.

1.2 CHALLENGES FOR MANAGING MULTI-MODULAR ADVANCED SMR PLANTS

Through economy of automation, a fully realized supervisory control system architecture can support the achievement of O&M cost performance that are comparable to large, stand-alone LWRs, relative to power output.

Two critical factors for the economic competitiveness of AdvSMRs are the up-front capital cost to construct the plant and the day-to-day cost of plant management (operations and maintenance). The former cost is primarily dependent on the size and complexity of the components that must be fabricated and the methods of installation. In this area, AdvSMRs have a clear advantage over large plants. The latter cost is strongly affected by the loss of economy of scale. The most significant controllable contributor to day-to-day costs arises from operations and maintenance (O&M) activities, which are heavily dependent on staffing size and plant availability. Efficient, effective operational approaches and strategic maintenance can help contain these costs and ensure economic viability.

The operation of a nuclear power plant is labor intensive. The O&M staff at a plant is composed of operator teams for each shift at each unit, and on-site maintenance personnel can involve a large number of technicians and specialists. The current industry average for O&M staff is roughly one person per every 2 megawatts of generated power. Existing regulations [10CFR50.54(m)(2)(i)] also establish minimum licensed operator and senior operator staffing requirements for each reactor unit. These staffing requirements are primarily based on responses to transients and accidents. These requirements are based on traditional operational models and limited automation. Without a significantly higher degree of automation than is customary for legacy nuclear power plants, high staffing levels relative to unit power production will pose the threat of unsustainable O&M costs for AdvSMRs.

Concepts for multi-unit AdvSMR plants can involve shared resources and systems among units to further reduce the up-front costs. This degree of sharing can range from minor support or auxiliary systems (e.g., emergency coolant tanks, control stations, and backup electrical power) to major primary or secondary systems (e.g., turbine-generators coupled with two or more units). Depending on the nature and degree of sharing among modules, there may be significant dynamic coupling that must be taken into account within the operational controls for the plant.

Unconventional and/or reconfigurable balance of plant arrangements may pose control challenges due to effects of operating mode transitions or dynamic coupling among interconnected systems. In-service reconfiguration of equipment lineups and flow interconnections to support product stream transitions can lead to significant transients. Propagation effects from dynamic coupling of different production systems (e.g., turbine-generator for electricity, thermal systems for desalination or hydrogen production) can lead to adverse feedback of downstream upsets. In addition, without automation, staffing demands for manual reconfiguration can be substantial. Integrated process diagnostics and intelligent control can enable automatic reconfiguration of balance of plant while anticipating downstream upsets and limit the impact of transients.

Fulfilling the goals of AdvSMR deployment depends on the resolution of technical challenges related to plant management complexity and unique operational conditions. The challenges include cost-effectiveness of plant management and optimization of operation. ICHMI technologies provide the foundation for what is the equivalent of the central nervous system of a nuclear power plant. Therefore, innovative use of intelligent automation can have a significant impact on resolution of challenges specific to AdvSMRs.

In summary, staffing, which is a large part of O&M costs, can be made comparable to or reduced compared to large LWRs. The following staffing areas will be reduced through the use of supervisory control:

Licensed operators

- More intelligently organized information and supervisory control can reduce the number of licensed operators required to safety operate the plant and to respond to transients/accidents

Roving operators

- The increased number of instrumented and visual displays can reduce the number of roving operators required by directing those operators to specific components for observation

Maintenance

- The significant increase in the number of components at a plant site (i.e., all reactor modules) would be expected to significantly increase the maintenance staffing requirements. However, the use of predictive monitors and a controlled realignment of equipment via the supervisory control system can allow for scheduled maintenance at a consistent pace. This condition can allow a smaller maintenance staff for the site because of a more efficient use of staff.

1.3 MOTIVATION FOR SUPERVISORY CONTROL SYSTEM DEVELOPMENT

Modern nuclear power plants incorporate greater automation but still rely on human interaction for supervision, system management, and operational decisions. More importantly, the human is also given the responsibility to serve as the last line of defense should ICHMI system failure prevent automatic plant protective measures from actuating, particularly in the case of prospective common cause failures that could disrupt multiple safety-related systems. This operational approach is acceptable for large nuclear plants because of the ability to defray personnel costs against the significant per-unit power output. In contrast, the AdvSMR imperative to control O&M costs by achieving reduced staffing implies the need for highly automated plant control with greatly reduced reliance on on-site highly skilled staff for interactive operational control under normal conditions and immediate intervention for event management.

Highly automated intelligent control involves more than simple automation of routine functions. It implies the detection of conditions and events, determination of appropriate response based on situational awareness, adaptation to unanticipated events or degraded/failed components, and reevaluation of operational goals. To enable plant operations based on a reduced staff, the control system for an AdvSMR must be capable of fulfilling these higher level supervisory and decision functions. The automation and intelligence incorporated in the AdvSMR control system can range from automated control systems that perform simple transitions among predefined operational strategies and functional configurations based on detection of triggering events to nearly autonomous control systems that can perform control, detection, decision, reconfiguration, and self-maintenance independently based on human permissives.

Unfortunately, highly automated, intelligent control capabilities have not been demonstrated for nuclear power plant operations and there is limited experience in other application domains. Supervisory control provides a means for the integration of control, decision, and diagnostics to support extensive automation. The targets for automation include operational management of highly complex plants, dynamic management and control of multiple product streams from a plant, and coordinated management of multiple modules. Specifically, control strategies and methods need to be developed within a flexible functional architecture to supervise multi-unit plants, accommodate shared systems or resources, and enable flexible co-generation operational regimes. Consequently, the Supervisory Control project was initiated to proceed with development and demonstration of the architectural framework and foundational modules that are needed to facilitate the integration of control, decision, and diagnostics to support the necessary level of automation.

1.4 IMPLICATIONS OF A SUPERVISORY CONTROL SYSTEM ON REACTOR OPERATIONS

Advances in technology and new levels of automation have provided positive effects in economics and safety. However, operational experience, research investigations, incidents, and occasionally accidents associated with automation on commercial jet transports have shown that new and sometimes surprising problems have arisen as well [2].

Breakdowns in the interaction between human operators and automated systems have created new and sometimes serious problems. Breakdowns surprise both users and designers.

- The automation must be observable to operators, and it needs to act in predictable ways. System operators are surprised when confronted with unpredictable and difficult to understand system behavior in the context of ongoing operations.

- The goal of designers is to make automated system team players, where human and machine agents are together as part of one system. System designers are surprised to find new problems that concern the coordination of people and automated systems when unexpected consequences occur because their automated systems failed to work as team players.

Automation is meant to improve operational efficiency and precision, but enhanced autonomy and authority of advanced automation has given rise to the unexpected problem of *communication with machines* rather than about its operations. This has occurred because "advanced automation can initiate actions without immediately preceding or directly related operator input (i.e. autonomy), and it is capable of modulating or overriding user input (i.e. authority)" [3].

The terms “automation surprises,” “lack of mode awareness,” or “mode confusion” reflect a misunderstanding of the current and future status and behavior of the automation. Such *lack of mode awareness* can occur due to various factors, including [3]

- inadequate feedback on system activities and
- gaps or misconceptions in knowledge and understanding of the automation.

Automation surprises begin with miscommunication or erroneous assessments between the automation and users, which lead to a gap between the user's understanding of what the automated systems are set up to do, what they are doing, and what they are going to do.

The evidence shows strongly that the potential for automation surprises is greatest when the following three factors converge [2]:

1 automated systems act on their own without immediately preceding directions from their human partner,
2 gaps in users' mental models of how their machine partners work in different situations, and
3 weak feedback about the activities and future behavior of the agent relative to the state of the world.

In most cases, breakdowns in coordination between operators and automation do not result in events with significant consequences. Occasionally, however, breakdowns in coordination may spiral toward disaster—referred to as the *going sour* accident. In this general class of accidents, an event occurs or a set of circumstances comes together that appears to be minor and unproblematic, at least when considered in isolation. This event triggers an evolving situation that is, in principle, possible to recover from. Nevertheless, through a series of commissions and omissions, erroneous assessments, and miscommunications, the human-automation team manages the situation into a serious and risky incident or even accident. In effect, the situation is managed into hazard.

Fortunately, going sour accidents are relatively rare, even in very complex systems. In a nuclear power plant, the going sour progression should be blocked because of two factors:

1. the protection system will terminate a going sour progression of an automated control system, and

2. the protection and control systems are independent, which prevents the going sour progression initiated in the control system from affecting the operability of the protection system.

The primary lesson from careful analysis of incidents and disasters in a large number of industries is that going sour accidents represent a breakdown in coordination between people and technology [4]. People cannot be thought about separately from the technological devices that are supposed to assist them. The key principle is that technology cannot be considered in isolation from the people who use and adapt it [5].

At the broadest level, researchers have identified a few basic human-centered strategies that organizations can follow in an effort to increase the human contribution to safety:

- increase the system's tolerance to errors,
- avoid excess operational complexity,
- evaluate changes in technology and training in terms of their potential to create specific kinds of human error,
- increase skill at error detection by improving the observability of state, activities, and intentions, and
- invest in human expertise.

Appropriate design should assume the existence of error, it should continually provide feedback, it should continually interact with operators in an effective manner, and it should allow for the worst of situations [4].

The likelihood of unintended consequences can increase when designers [6] do the following:

- oversimplify the pressures and task demands from the users' perspective,
- assume that people can and will call to mind all relevant knowledge,
- are overconfident that they have taken into account all meaningful circumstances and scenarios,
- assume that machines never err,
- make assumptions about how technology impacts on human performance without checking for empirical support or despite contrary evidence,
- define design decisions in terms of what it takes to get the technology to work,
- sacrifice user-oriented aspects first when trade-offs arise,
- focus on building the system first, and then trying to integrate the results with users.

Higher levels of system autonomy, authority, complexity, and coupling increase the need for communication and coordination (observability) between humans and machines. These properties are defined as [3] follows.

> *Authority* refers to the power to control a process. The level of authority of an automated control system has implications for the role and responsibility assigned to its human operator.[*]
>
> *Autonomy* denotes a system's capability to carry out sequences of actions without requiring (immediately preceding) operator input. In other words, autonomy refers to a system's level of independence from the human user for some specific task.

[*] *Authority* also implies that the operator has the means to instruct, redirect, and if need be "'escape" from the automation when deemed necessary. Having available the nominal means to instruct or escape is not sufficient. These mechanisms have to be usable under actual task conditions of multiple tasks, a dynamic world, and multiple data sources competing for attention. If, for example, control over the automation can be achieved only by means of a sequence of rarely executed actions that may require the diversion of attention away from critical system parameters in an escalating problematic situation, the automation is only a burden and not a resource or support.

System complexity is determined by the number of system components and especially by the extent and nature of their interactions.

Coupling refers to the potential for an event, fault, or action to have multiple cascading effects.

Observability refers to processes involved in extracting useful information, which are key to supporting human-machine communication and system awareness. System awareness is the prerequisite for realizing the need for intervention with system activities that are not desirable or may even be dangerous.

Increasing autonomy and authority of machine agents without an increase in observability leads to automation surprises. Data on automation surprises on commercial jet transports has shown that crews generally do not detect their miscommunications with the automation from displays about the automated system's state, but rather only when aircraft behavior becomes sufficiently abnormal.

This result is symptomatic of low observability. Note that observability is distinct from data availability, which refers to the mere presence of data in some form in some location.

In most cases, automation silently compensates for deviations from preferred parameters, leaving operators unaware of the developing trouble until the automation nears the limits of its authority or capability to compensate. When automation is working at the extreme ends of its envelope or authority, improved displays and warnings can be used to indicate

- when the automation is having trouble handling the situation,
- when the automation is taking extreme action or moving towards the extreme end of its range of authority, and
- when agents are in competition for control.

Operators will require feedback on how the automation is performing. Improperly designed feedback that talks too much or too soon or that is too silent, speaks up too little or too late as automation moves towards authority limits does not increase operators observability. In short, errors in designing feedback include

- nuisance communication,
- excessive false alarms, and
- distracting indications.

One cannot improve feedback or increase observability by adding a new indication or alarm to address cases one at a time as they arise. A piecemeal approach will generate more displays, more symbolic coding on displays, more sounds, more alarms. More data will be available, but this will not be effective feedback because it challenges the ability to focus on and digest what is relevant in a particular situation. Improved feedback requires an integrated solution.

Giving users visibility into the machine agent's reasoning processes is only one factor in making machine agents into team players. Without also giving the users the ability to direct the machine agent as a resource in their reasoning processes, the users are not in a significantly improved position. They might be able to say what's wrong with the machine's solution, but remain powerless to influence it in any way other than through manual takeover. In order to make use of this potential, the users need to be given the authority and capabilities to make those decisions. This means giving them control over the problem solution process.

A commonly proposed remedy for this is to allow users to interrupt the automated agent and take over the problem in its entirety in situations where users determine that the machine agent is not solving a problem adequately. Thus, the human is cast into the role of critiquing the machine, and the joint system operates in essentially two modes: (1) fully automatic or (2) fully manual. The system is a joint system only in the sense that either a human agent or a machine agent can be asked to deal with the problem, not in the more productive sense of the human and machine agents cooperating in the process of solving the problem. This method, which is like having the automated agent say "*either you do it or I'll do it*," has many obvious drawbacks. Either the machine does the entire job without benefiting from the practitioner's information and knowledge, despite the brittleness of the machine agents, or the user takes over in the middle of a deteriorating or challenging situation without the support of cognitive tools. It has been shown that this is a poor cooperative architecture. Instead, users need to be able to continue to work with the automated agents in a cooperative manner by taking control of the automated agents [2].

The last area for investment in the interest of improving the human contribution to safety is human expertise. One of the myths about the effect of automation on human performance is that as investment in automation increases, less investment is needed in human expertise. In fact, many sources have shown how increased automation creates new and different knowledge and skill requirements [2].

1.5 REFERENCES – CHAPTER 1

1 M. Antkowiak and M. Ruth, *Summary Report of the INL-JISEA Workshop on Nuclear Hybrid Energy Systems*, Technical Report, NREL/TP-6A50-5560 (July 2012).

2 D. D. Woods, N. B. Sarter, I. N. Starter, and R. Amalberti, "Learning from Automation Surprises and 'Going-Sour' Accidents," Ohio State University, Institute for Ergonomics, Cognitive Systems Engineering Laboratory, National Aeronautics and Space Administration National Technical Information Service, distributor (1998).

3 N. B. Sarter and D. D. Woods, "Team Play with a Powerful and Independent Agent: A Full-Mission Simulation Study," *Human Factors*, **39**(4), 553–569 (December 1997).

4 D. A. Norman, "The 'Problem' of Automation: Inappropriate Feedback and Interaction, not 'Over Automation'," *Philosophical Transactions of the Royal Society of London, B*, **327**, 585–593 (1990).

5 E. Hutchins, "How a Cockpit Remembers its Speeds," *Cognitive Science*, **19**, 265–288 (1995).

6 N. B. Sarter, D. D. Woods, and C. E. Billings, "Automation Surprises," *Handbook of Human Factors and Ergonomics*, 2nd edition, G. Salvendy (Ed.), Wiley, 1997.

2. SUPERVISORY CONTROL SYSTEM ARCHITECTURE BACKGROUND

Modern control systems for mission-critical industries such as aerospace, nuclear, chemical, and defense require multidisciplinary system engineering during all phases of the project. These disciplines may include structural, mechanical, chemical, nuclear, electrical, electronic, algorithms, communications, software, and computation among others.

For example, embedded real-time software has experienced an exponential growth in scale for various industries and applications. NASA has commissioned studies on the growth in scale of software requirements, software complexity, managing complexity, life cycle management, software testing, verification, and validation [1]. The F-35 Joint Strike Fighter weapon systems, flight control, and propulsion control systems utilize approximately 5.7 million lines of embedded software code [1]. Challenges of cost, schedule, and performance create conditions for prioritization of software code production versus requirements, architecture, and design. Discipline and self-enforcement for proper compliance are challenging to maintain due to reasons such as the difficulty in quantifying benefits and the delayed results of actions in software development.

2.1 STATE-OF-THE-ART OF AUTONOMOUS CONTROL ARCHITECTURES

Architectures, in general, have distinct features that lead to different properties, which then lead to support specific capabilities. The choice of features is often made by following explicit methodological assumptions, driven by the domains and environments for which the design will be implemented. The variety of choices leads to variety of system architectures that can be found.

2.1.1 Early Autonomous Architectures

There have been a plethora of architectures developed for automation systems. For early automation systems, the dominant view was that the control system could be broken down into three functional elements:

1 sensing system,
2 planning system, and
3 execution system.

The sensing system, that is, the data acquisition system, translates raw sensor data into a world model. The planner takes the world model and generates a plan based on predefined goals. The execution system then takes the plan and generates the actions it prescribes. This basic architecture was called *sense-plan-act* (SPA) or *sense-plan-execute* (SPE) [2].

2.1.2 Subsumption Architecture

In the mid-1980's, Brooks introduced the *Subsumption architecture* for autonomous robots [3]. The Subsumption architecture was the first known departure from SPA.

The Subsumption architecture was built in layers. Each layer gives the system a set of pre-wired behaviors. The higher levels build upon the lower levels to create more complex behaviors. The behavior of the system as a whole is the result of many interacting simple behaviors. The layers operate asynchronously.

The layers of the Subsumption architecture are composed of networks of *finite state machines* augmented with timers, which enable state changes after preprogrammed periods of time. Each augmented finite state

machine (AFSM) has an input and output signal. When the input of an AFSM exceeds a predetermined threshold, the behavior of that AFSM is activated (i.e., the output is activated). The inputs of AFSMs come from sensors or other AFSMs. The outputs of an AFSM are sent to the agent's actuators or to the inputs of other AFSMs.

Each AFSM also accepts a suppression signal and an inhibition signal. A suppression signal overrides the normal input signal. An inhibition signal causes output to be completely inhibited. These signals allow behaviors to override each other so that the system can produce *coherent* behavior.

Subsumption achieved dramatic early success in the area of collision-free robot navigation. While, SPA-based robots were pondering their plans, Subsumption-based robots were easily performing the tasks in normal office environments with many obstacles.

The Subsumption architecture reached a pinnacle with a robot called *Herbert*, which was programmed to find and retrieve soda cans in an office environment [4]. While Herbert exhibited impressive capabilities—even by today's standards—it also represented the limits of what could be achieved with Subsumption. One obvious shortcoming of this robot was that it was unreliable in that it could not perform a complete can-retrieval task flawlessly.

One possible cause of Subsumption's *capability ceiling* is that the architecture lacked mechanisms for managing complexity. It was later concluded that the major problem with the architecture was lack of modularity, which ultimately resulted in interference of upper layers with the internal functions of lower-level behaviors. Because of that, lower-level behaviors could not be designed independently, and they became increasingly complex. This also meant that even small changes to low-level behaviors required a complete redesign of the controller [5].

2.1.3 T/R-III Architecture

The years following the introduction of Subsumption saw a profusion of new robot control architectures, typically as a direct response to Subsumption's shortcomings [6–11].

One successful architecture was T/R-III, which had a layered design like Subsumption. However, unlike Subsumption, T/R-III embraced abstraction rather than rejecting it. In Subsumption, higher-level layers interfaced with lower-level ones by *suppressing* the results of the lower-level computations and superseding their results, However, in T/R-III, higher-level layers interfaced with lower-level layers by *providing input* or *advice* to the lower-level layers. In other words, layers in T/R-III provided layers of *computational abstraction* as well as layers of functionality [12, 13].

Autonomous robots that had the T/R-III architecture were among the first ones that were capable of reliably performing a more complex task than simply moving from place to place. However, they had one serious drawback: they were not *taskable*, that is, it was not possible to change the task they performed without rewriting their control program.

2.1.4 3T, SSS and ATLANTIS Architectures

At least three different groups of researchers working more or less independently came up with similar solutions to this problem [14–16]. All three solutions that were developed after the Subsumption model consisted of control layers that were composed of three main elements:

1 a reactive feedback control mechanism,
2 a slow deliberative planner, and

3 a sequencing mechanism that connected the first two elements.

Connell's sequencer was based on Subsumption [14]; Bonasso used Kaelbling's *REX/GAPPS* system [17], and Gat's was based on Firby's *Reactive Action Packages* (RAPs) system as described in his 1989 thesis [18].

Aside from the technical advances, there are two items of historical interest in Firby's thesis: The first is that the architecture was later renamed *reactive execution* rather than *reactive planning*, which signified an obvious departure from the SPA tradition. The second is that it contained the earliest description of the *three-layer architecture* that has become the *de facto* standard [18].

This RAP-based three-layer architecture has come to be called 3T [19], Connell's Subsumption-based architecture was called SSS, and Gat's architecture was called ATLANTIS.

The main differences between 3T and ATLANTIS were the following:

1. ATLANTIS used a different representation in its sequencing layer, one designed more for programming convenience than for use as a planner representation,

2. The sequencer controlled the operation of the planner rather than vice versa.

ATLANTIS also extended the RAPs action model to use continuous real-time processes rather than atomic operators, which later became the *de facto* standard.

2.1.5 RA Architecture

The *Remote Agent* (RA) architecture was developed and tested as part of the Deep Space 1 mission, which is illustrated in Fig. 1. The RA architecture included the *Mission Manager* (MM), *Planner/Scheduler* (PS), *Smart Executive* (EXEC) and *Mode Identification and Reconfiguration* (MIR) modules in a relatively flat structure, where modules are allowed to interact in a matrix composition [20]. The MM and the P/S modules are shown as separate objects in Fig. 1, while in fact, they perform a tightly coupled function. This coupled functionality results from that fact that the MM maintains the mission profile that guides the planning for the mission lifetime, whereas the P/S develops flexible, concurrent, temporal plans for a time horizon—typically two weeks—based on goals from the mission profile supplied by the MM. The plans are provided to the EXEC module, which is a control manager that executes the sequence of activities and reacts to failed responses. It is responsible for coordinating resource management, action definition, fault recovery, and configuration management. The MIR module is a model-based component that monitors the condition of the spacecraft, identifies failures, and provides recovery procedures to the EXEC. On request from the EXEC, the MM and P/S will develop a revised plan to account for failures or recoveries. Through its multi-module approach, the RA is able to provide a *reactive response* to failures (EXEC) and a *deliberative response* to events (P/S). The reactive response provides real-time action to address the immediate consequences of failures whereas the deliberative response (i.e., replanning) provides the capability to assess the impact of failures or events on the mission goals, and then determine how to proceed with the mission while accommodating those conditions.

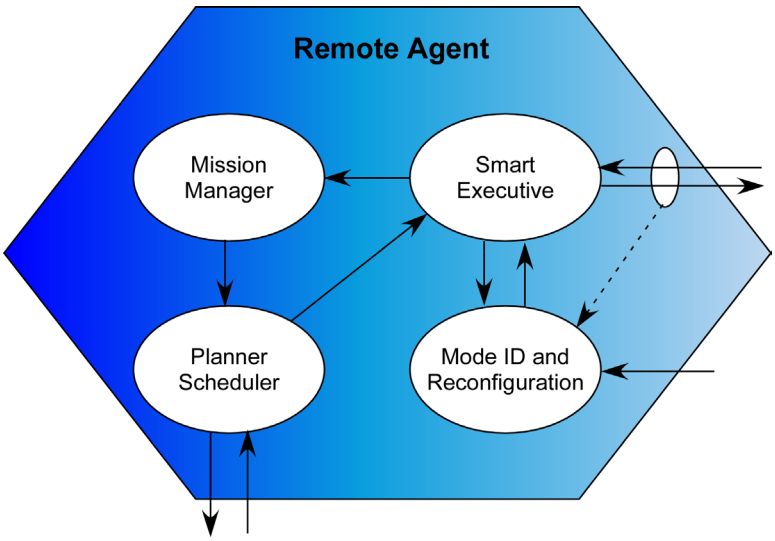


Fig. 1. Remote agent (RA) architecture developed for Deep Space 1.

2.1.6 CLARAty Architecture

The *Coupled-Layer Architecture for Robotic Autonomy (CLARAty)* architecture was designed for improving the modularity of system software while tightly coupling the interaction of autonomy and controls, in which the planner and executive layers were lumped into one *decision layer* [21]. The decision layer interacted with a separate functional layer at all levels of system granularity—as shown in Fig. 2 [22]. The functional layer was an object-oriented software hierarchy that provided basic capabilities of system operation, resource prediction, state estimation, and status reporting. The decision layer utilized these capabilities of the functional layer to achieve goals by expanding, ordering, initiating and terminating activities. The CLARAty architecture implemented both declarative and procedural planning methods.

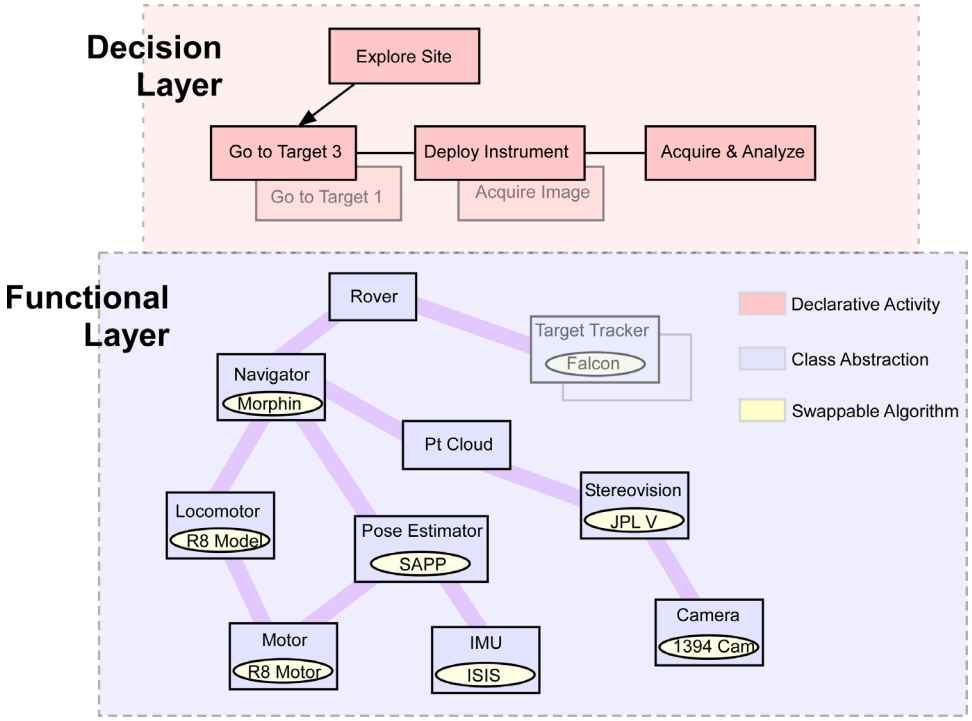


Fig. 2. The overall CLARAty architecture with a declerative-based decision layer and procedural-based functional layer.

The Mars Technology Program has funded development of autonomous control architecture to support the *Mars Exploration Rover* (MER) mission. The CLARAty software environment supports autonomy for the rovers *Spirit* and *Opportunity*. The dual layer architecture of CLARAty is illustrated in Fig. 3. The CLARAty architecture provides an upper (decision) layer for artificial intelligence (AI) software and a lower (functional) layer for controls implementations. The development of CLARAty addresses the perceived issues with the three-tiered architecture, which is typical of robotic autonomy [21]. Those issues are the tendency toward a dominant level that depends on the expertise of the developer, the lack of access from the deliberative or planner level to the control or functional level, and the difficulty in representing the internal hierarchy of each level—e.g., nested subsystems, tress of logic, and multiple time lines and planning horizons—using this representation. In one sense, the CLARAty architecture collapses the planner and executive levels, which are characterized by high levels of intelligence, into the decision layer. Essentially, the deliberative and procedural functionalities are merged into an architectural layer that parallels the functional layer and provides a common database to support decision-making. Additionally, a system granularity dimension is maintained to explicitly represent the system hierarchies of the functional layer and the multiple planning horizons of the decision layer.

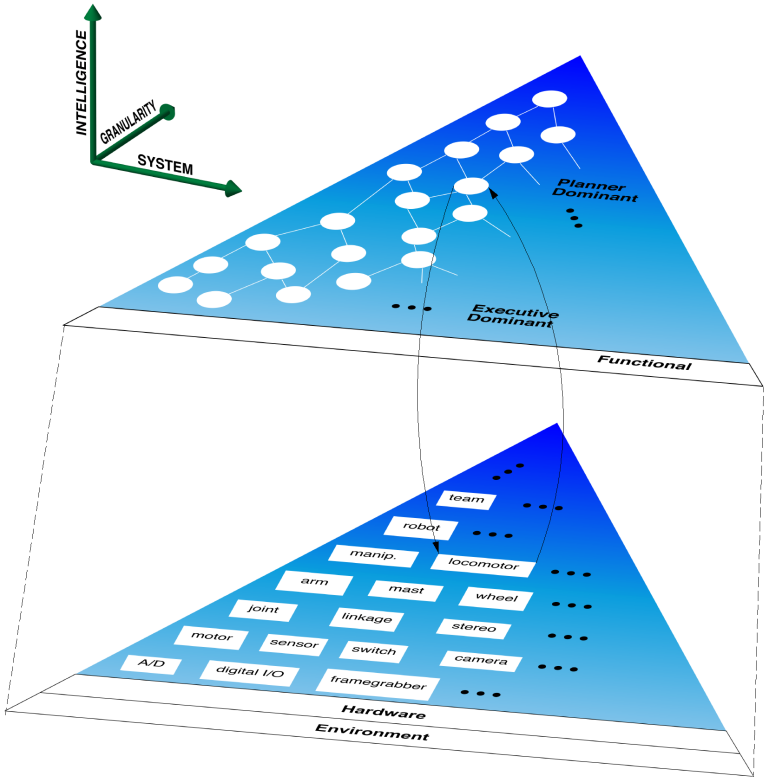


Fig. 3. Decision and functional layers in the CLARAty architecture.

2.1.7 Earlier Supervisory Control Architectures Proposed for Nuclear Power Plants

There is an architectural approach for nearly autonomous control systems that has been applied through simulation for nuclear power specific applications. As part of research to support advanced multi-modular nuclear reactor concepts, such as the International Reactor Innovative and Secure (IRIS) and the ALMR, a supervisory control system architecture was devised [23–25]. This approach provides the framework for autonomous control while supporting a high-level interface with operations staff who can act as plant supervisors. The final authority for decisions and goal setting remains with the human but the control system assumes expanded responsibilities for normal control action, abnormal event response, and system fault tolerance. The autonomous control framework allows integration of controllers and diagnostics at the subsystem level with command and decision modules at higher levels.

The autonomous control system architecture shown in Fig. 4 is hierarchical and recursive. Each node in the hierarchy (except for the terminal nodes at the base) is a supervisory module. The supervisory control modules at each level respond to goals and directions set in modules above it within the hierarchy and to data and information presented from modules below it within the hierarchy. Each module makes decisions appropriate for its level in the hierarchy and passes the decision results and necessary supporting information to the functionally connected modules.

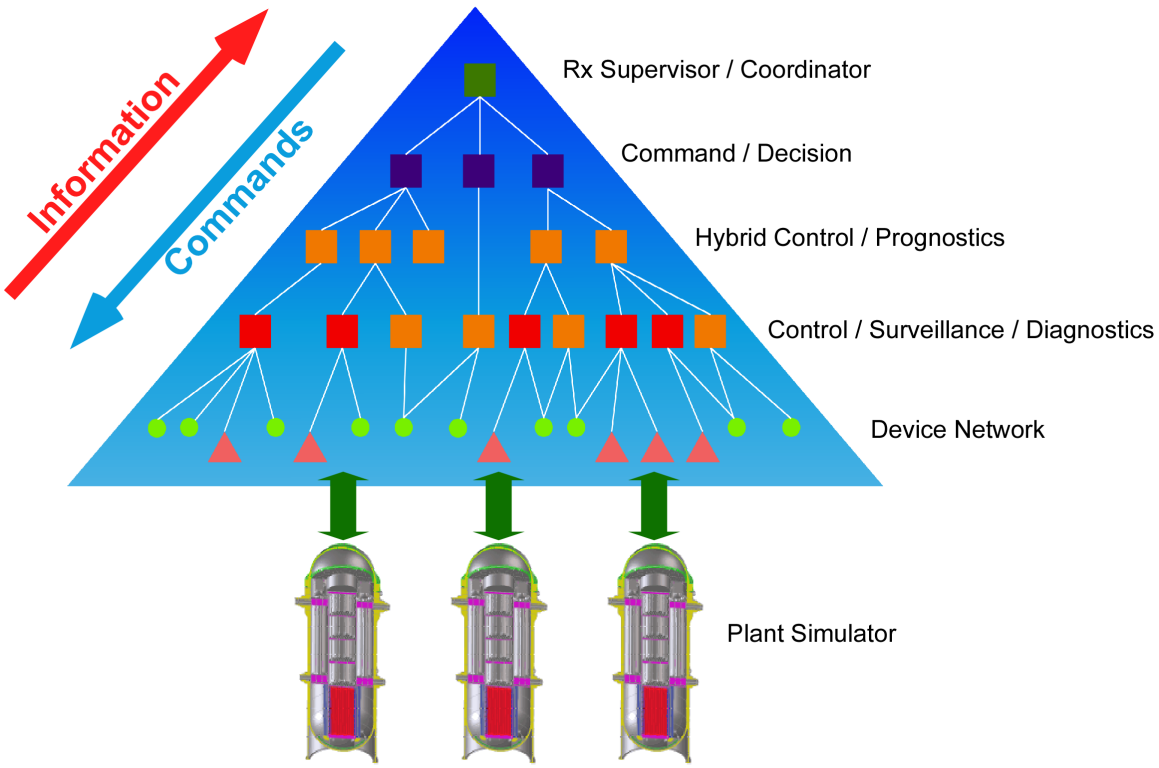


Fig. 4. Supervisory control architecture proposed for multi-module nuclear power plants.

2.1.8 The Anatomy of the Three-Layer Architecture and the Role of Internal State

These observations naturally lead to the following questions [26]:

- *Why do so many independently designed architectures turn out to have such a similar structure?*
- *Are three components necessary or sufficient, or is number three a coincidence?*

It was shown that the three distinct layers of functionality was essentially a result of methods to manage the *internal state* information [26]. Time-consuming computations, such as *decision making* and *planning*, require that certain data be stored (i.e., the internal state) during complex mathematical calculations. Problems arise when the stored value deviates significantly from the actual process value at the end of the computation prior to an action.

The natural solution, obviously, is to eliminate the use of internal states. However, this requires fast sampling, high bandwidth, and high computational power. Technological advances pretty much eliminate the first two problems; however, the latter may still be an issue for *Non-deterministic Polynomial-time hard problems* (i.e., *NP-hard problems*), such as global optimization calculations that may require extensive search for minima. These restrictions may further be compounded with financial as well as physical space constraints. Therefore, the technology ceiling should always be taken into account in complex, large-scale systems.

From the internal states perspective, three-layer architectures—as shown in Fig. 5—organize algorithms according to the following principles [26]:

1 the functional layer (also called *controller* layer) contains no internal state,
2 the coordination layer (also called *sequencer* layer) contains memory about the past, and
3 the organization layer (also called *deliberator* layer) contains memory about the future.

The functional layer consists of one or more threads of computation that implement a series of feedback control loops, the number of which can be quite large for a complex, large-scale system. These loops include reactive control algorithms, which map sensors directly onto actuators with little or no internal state.

The coordination layer is an intermediate level that essentially serves two functions:

1 transfer data from the functional layer to the organization layer: encode sensory data in a form consistent with the language of the organization layer, and

2 transfer data from the organization layer to the functional layer: decode instructions from the organization layer into specific actions to be performed by the coordination layer.

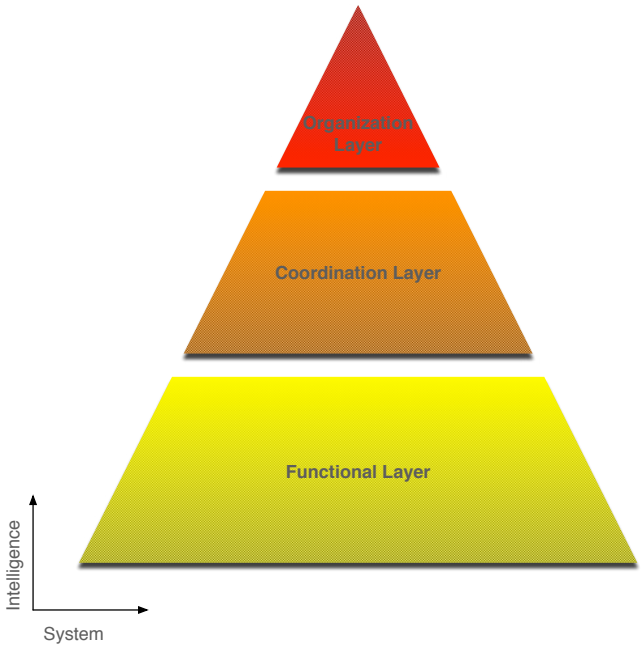


Fig. 5. Structure of the hierarchy for the supervisory control architecture.

The coordination layer contains algorithms for governing routine sequences of activity, which rely extensively on internal state, but they typically do not perform time-consuming searches.

The organization layer sits at the top of the computational hierarchy and is responsible for performing more time-consuming calculations. The output of these calculations—such as decision-making planning, and scheduling—generates instructions that define the actions to be taken by lower layers of the hierarchy. The decision-making algorithms can be rule based, which tend to generate faster results, or based on a search algorithm.

The three-layer architecture essentially provides a graded abstraction at each layer. The premise is that algorithms at one layer provide effective computational abstractions for constructing interfaces to algorithms of the next higher layer.

The layered structure results in successive delegation of duties from higher levels to lower levels; hence, the number of distinct tasks increases as one goes down the hierarchy. Higher levels are concerned with slower aspects of system's behavior while responsible for planning with a longer time horizon. In a typical hierarchical structure, intelligence increases while precision decreases in higher levels [27, 28]. Therefore, it is common that while lower layers employ numerically intensive calculations, higher layers resort to symbolic decision making methods.

2.1.9 Autonomous Control in Other Industries

During the architecture development task, the project staff interacted with other industries to investigate the state-of-the-art of automation in other industries. The staff contacted a number of corporations from chemical plants to coal-fired plants. Tennessee Valley Authority (TVA) responded positively to ORNL's requests for touring the main control rooms of their power generation stations.

2.1.9.1 Control of Fossil Power Plants

Kingston Fossil Plant—also called Kingston Steam Plant—is located on Watts Bar Reservoir on the Tennessee River near Kingston, Tennessee. At the time it was finished in 1955, Kingston was the largest coal-burning power plant in the world, a distinction it held for more than a decade.

Electricity is produced at each of Kingston's nine coal-fired units individually by heating water to produce superheated steam. Kingston Plant generates about 8 billion kW-h of electricity a year.

Bull Run Fossil Plant is located on Bull Run Creek near Oak Ridge, Tennessee. It is the only single-generator coal-fired power plant in the TVA system. When the generator went into operation in 1967, it was the largest in the world in the volume of steam produced. Bull Run also operates at supercritical pressure generating about 6 billion kW-h of electricity a year. It has been ranked the most-efficient coal-fired plant in the nation 13 times and is consistently in the top five each year.

As part of the ORNL supervisory control research for future AdvSMRs, some ORNL personnel visited and toured the TVA Kingston and Bull Run coal steam-generating plants to examine their current state of controls and instrumentation. Several key findings were identified.

The TVA power load center in Chattanooga directs the power generation for the plant total and also for each generation unit. This is implemented either with a direct data link from the TVA power load center providing a setpoint to the local plant controls (Automated Generation Control) or with the data provided to the plant operator who manually follows the TVA request. The local plant does not perform any decision making about the makeup of each generation unit to the generation total. This practice defines the control decision-making boundary for each power generation unit and for the total plant to accept and fulfill the utility power demand request. The TVA power load center decision-making is based on economics, load demand, weather, and host of other factors.

The Kingston and Bull Run plants demonstrated different levels of modern control and operator interfaces. The Bull Run plant was converted to the Emerson Ovation Distributed Control System (DCS) in 1998 with limited computer-based operator interfaces. Bull Run relied on significant levels of manual operation and decision-making. The Kingston plant was also converted to an Emerson Ovation Distributed Control System (DCS) to replace previous aging DCS systems. This DCS platform has a

standard suite of software functions, control, and operator interfaces with a large global installation experience. Most of the Kingston generation unit control rooms had a mixture of computer-based operator interfaces and legacy operator interface indicators and devices. Kingston unit #9 was the last upgrade with a control room that did not have any legacy operator interfaces but consisted of all computer-based operator interfaces.

One additional aspect of the supervisory control system to consider is that a utility control center will direct the electrical output of each generator at a plant. For the Kingston Fossil Plant, the TVA Control Center in Chattanooga, Tennessee, gives separate, independent control signals to each of the plant's nine coal-fired units. In some cases, the signals directly provide set point values to the digital control systems, while in others the signal is displayed to the plant operator, who then manually enters the set point. In either case, the result is that TVA central control in Chattanooga, Tennessee, acts as the supervisory controller for the Kinston Fossil Plant. In fact, central control is providing the supervisory control function to all generators in the TVA part of the grid—coal plants, gas turbine plants, hydroelectric plants, nuclear plants, etc. Central control, however, does not provide such set points to privately owned generators, such as privately owned renewable power generation sources, including wind, solar, geothermal, etc. Federal law is written so that a non-utility must buy renewable from the generator.

The Kingston plant technical staff discussed diagnostics and fault detection experiences. The common theme was that proper sensor installation and maintenance was vital to maintaining the capability. If proper sensor installation and maintenance were not followed, then the desired fault detection and diagnostics were not realized.

The following is a summary of findings based on ORNL staff's observations and interactions with the site personnel.

1 The local generation and plant control systems receives a generation request from the utility (i.e., MWe to the grid). The utility can limit the request based on status of the plant.

2 The current state-of-the-art in modern DCSs for coal steam-generating plants and other types of plants offers a valuable foundation of capability, reliability, and experience that could be leveraged for future aSMR control system concepts. For example, DCS capabilities for operator interfaces could be leveraged for future aSMR concepts.

3 A reduction in maintenance and operations costs is possible with successful fault detection and diagnostics.

2.1.9.2 High Flux Isotope Reactor (HFIR)

The High Flux Isotope Reactor (HFIR) is currently undergoing an analog-to-digital system upgrade of its control system. More specifically, the Wide Range Counting Channel (WRCC) System—one of the nuclear instrument systems that is used during startup to provide reactor control and indications of power and startup rate—is being upgraded in a phased approach [51].

This phased approach allows for the development, testing, and installation of the system on a step-by-step basis. Because technical specifications require only 2 of the 3 channels to be operational, only one channel would be replaced initially. This will allow the operations staff to gain experience with the new design, provide additional validation of the software through comparison with the analog system, and allow for any software corrections.

The WRCC system is in its final stage of pre-installation testing. The status of this control system, its capabilities as a supervisory control will be monitored and evaluated further during the next phase of this project.

2.2 CONSIDERATIONS ON SUPERVISORY CONTROL ARCHITECTURE

Experience with large-scale projects requiring significant systems engineering can determine key considerations for guidance in the construction of control system architecture. Jon Clauss with Lockheed Martin Aeronotics described this as "One of the biggest challenges is getting to a common understanding of what architecture contains and how to represent it" [29].

- *Architecture*: an arrangement of design elements and collaborations between those elements that satisfies the customer's requirements.

- System architecture exists in the context of a larger enterprise.

2.2.1 Functionality

The system functionality requirements will determine the system design and implementation. This leads to key questions to aid in defining the system architecture. The follow questions are not exhaustive but are suggestive of the proper level of scrutiny.

- Are the system and subsystem requirements properly defined?
- Are the goals and challenges understood?
- Do the requirements determine the level of automation?
- Is the desired level of system and sub-system autonomy understood?
- Are the operational requirements understood?
- Are commercial sensors available to meet the measurement needs and requirements?
- Are commercial actuators available that meet the requirements?

2.2.2 Performance and Stability

Performance may be defined as the ability to execute a defined task. Stability is a term used in the field of control systems to discuss the ability of a system to execute a task consistently without undesirable behavior despite variation in the conditions or disturbances. This leads to key questions to aid in defining the system architecture. The following questions are not exhaustive but suggest the proper level of scrutiny.

- Do the measurement sampling and control requirements necessitate hard real-time (time critical) or soft real-time (less time critical) [30]?

  Examples of real-time categories include sample times of <250 microseconds (~10 microseconds jitter), <100 milliseconds (~20 microseconds jitter), <1 second (~10 milliseconds jitter, or deviation from the desired cycle time), or >1 second. The functional requirements will determine multi-tasking demands, quantity of input/output (I/O), logic scan rates and determinism, and the quantity and type of signal processing algorithms.

  The complexity of the plant and system dynamics combined with performance and stability requirements determine the level of control law (algorithms and logic implemented in software) complexity, which drives the requirements complexity, design complexity, and the costs for validation and verification.

- The control performance requirements are driven by key system information. Is the system to be controlled inherently stable or unstable? Does the system have significant complex coupling dynamics? Is the system observable and controllable? Does the process have significant signal noise, uncertainties, and/or disturbances? Does the system have nonlinearities and/or time delays? Do sensors and actuators have nonlinearities such as dead zone, threshold, and hysteresis?

- Do reasonable dynamic models of the system exist for control design, validation, and verification? Is model order reduction needed? Some algorithm design techniques require high-fidelity dynamic models. Will a model-based development process be followed?

  Modern aerospace and defense projects typically follow a model-based development process (Fig. 6). A dynamic behavior model of subsystems and systems can be used to develop and test the control laws (algorithms and logic implemented in software), perform software-in-the-loop testing, and perform hardware-in-the-loop testing [31].

- Is the system multivariable in nature? The requirements must include stability margins for subsystem and system control. Complex multivariable algorithms require significant computation resources, strong determinism and synchronization, and a centralized or locally centralized organization of I/O, information, and processing [32].

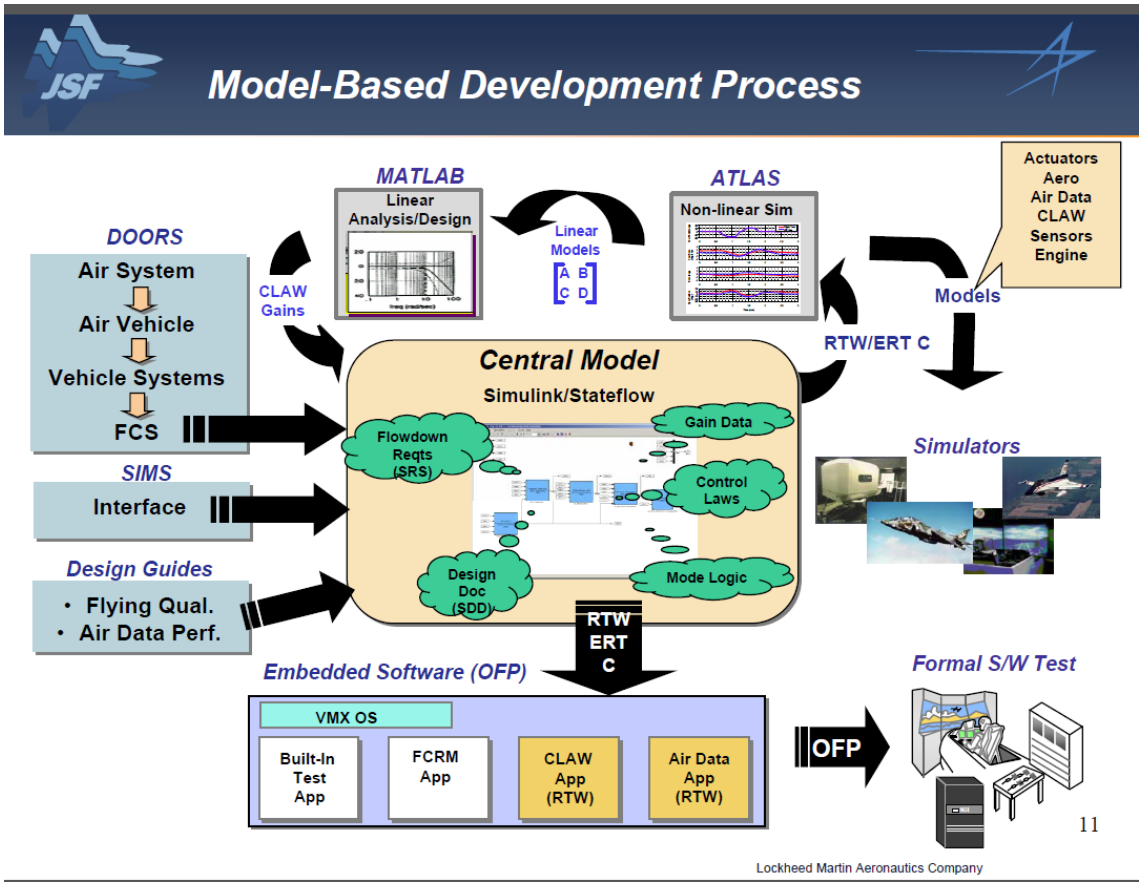


Fig. 6. Lockheed-Martin F-35 model-based development process.

- Do requirements demand custom hardware or will commercial off-the-shelf (COTS) offerings with proper software meet requirements? Do actuation and sensing devices provide appropriate performance for the control system? Sensing and actuation bandwidth must properly align with control bandwidth for proper performance and stability. Do actuation and sensing devices avoid nonlinearities such as limit cycling and saturation in the standard operating envelope?

  If redundancy and/or multichannel operation are required due to reliability requirements, the control algorithms must account for consequences such as non-minimal realization and mismatch of integrators for multiple channels [32].

2.2.3 Environment

The environment must be characterized for devices, sensors, and computation. This will determine the level of durability and environmental controls required. This can also direct durability requirements for harsh environments such as significant levels of radio frequency noise, electromagnetic interference, extremes of temperature, vibration, or radiation.

2.2.4 Communications

The architecture must support communications for field measurement, control, status, diagnostics, data collection, human interfaces, and plant-wide information. The quantity of data and the data sample rate must be clearly defined.

The communications architecture should consider proper segregation and independence for system reliability and fault tolerance. This could include location, electrical power, communication, software, and functional interaction. The system should avoid complexity to minimize the probability of undiscovered flaws, or the system should be testable to properly validate and verify the system integrity. Architecture and design decisions should reduce the potential for common mode failures that violate reliability requirements for single-point failures [33].

The control system communication network architecture and design should provide sufficient bandwidth for all desired and necessary data traffic. Additionally, the communication network and components must have requirements for significant bandwidth margin, network segregation, and component interaction behavior. For example, an event with variable frequency drive failures due to excessive network traffic occurred at Browns Ferry Nuclear Station, Unit 3 [34].

The control system communication system architecture and design should also include monitoring and diagnostics. The data traffic should be measured and tracked to determine the consumed bandwidth and the remaining bandwidth margin. Anomalous data traffic should trigger alerts. Communications errors (corruption, loss, delay, etc.) should be measured and tracked. In addition to the vendor-provided status indicators, the networked components should incorporate a separate heartbeat function via software to ensure correct communication behavior (jitter, delay).[*] Information can be combined to determine the health and status of the communication networks. For an analysis of communications error and methods of defense, see reference [35].

[*] A heartbeat is a signal or a message passed between cooperating processes to indicate proper operations. Heartbeat communication between cluster nodes can be used to eliminate a single-point failure.

2.2.5 Reliability

To achieve overall system reliability, all subsystems must fulfill their individual reliability budget. Mechanical systems, computing hardware, software algorithms, electronics, and electrical systems must all fulfill their reliability budgets. Components that do not meet their reliability targets require countermeasures including redundancy to provide a net component reliability that is acceptable. The control algorithms may be required to include features for redundancy, operating with different configurations of functioning hardware, and alternative control strategies. Various operation testing strategies, such as continuous monitoring/testing, initiated built-in-testing, commissioning testing, and others, may be foundational in achieving the desired system reliability.

All programs must determine an accepted method for determining the reliability and qualifying the reliability of components. This can be very challenging with complex systems [36]. One approach to improving reliability is the Safety Integrity Level (SIL), which is defined as the measure of the safety risk, or the Probability of Failure on Demand (PFD). SIL levels are determined for instrumentation using techniques such as Failure Modes, Effects, and Criticality Analysis (FMECA) and Proven-in-Use (also called Prior Use) historical use data [37]. The processes for software requirements, engineering, design, coding, and testing must follow established mission-critical practices and standards such as Capability Maturity Model Index, DO-178, and ISO 9001:2008 [38–39]. Requirements and design must prevent undesired combinational events from occurring (conflicting operator commands, command input validation, etc.) [40].

Distributed control architecture utilizes control solutions via local interactions only. Centralized control architecture utilizes control solutions that require global information and communication with other localities [41]. Decentralized or distributed control architectures generally exhibit stronger system fault tolerance because of less exposure to single-point total system failures [39]. Stability analysis research for interconnected dynamic systems leads to centralized and local architecture formulations.

2.2.6 Testability (Validation and Verification)

The system architecture and design must have the capability to perform system validation and verification and to properly commission the system. Analysis tools and methods must provide the capability to test and quantify system health and stability.

Experiences in the nuclear power industry indicate some key findings. End-to-end functional testing can only verify and validate the performance of a control system for the tested sets of conditions. Methodologies for improving test coverage of the hardware and software either after installation or in component testing are necessary to obtain the desired system reliability [38].

2.2.7 Maintainability

The system architecture and design must select vendor platforms, which determine choices such as proprietary versus industry standard versus open hardware and software. Vendor selection should include product flexibility, scalability, vendor stability, supply chain, obsolescence, and long-term planning [36]. System complexity can challenge long-term maintainability.

The system architecture and design should reflect if a vendor-centric or asset owner-centric approach to system responsibility will be pursued. A vendor-centric system responsibility model requires the vendor to provide rigorous support through the design, construction, installation, and long-term support phases. The asset owner-centric approach requires the asset owner to assume primary responsibility for the design, construction, installation, and long-term support.

The total life cycle costs should be determined (design, construction, installation, operational, maintenance, future upgrades, and others).

Mission critical software, which can be defined as software applied to real-time hardware for the purposes of controlling mission-critical processes, has experienced escalated growth in lines of code, distributed architectures, and complexity. This has created a significant burden on the Post-Deployment Software Support (PDSS) process. The Embedded Computer Resource Support Improvement Program (NASA) studied the PDSS process and opportunities for improvement. PDSS objectives were determined to reduce the life cycle cost, improve the flexibility of software updates, improve the development, test, and documentation capability, and ensure process integrity [42].

NASA has commissioned studies on the growth in software requirements, software complexity, managing complexity, life cycle management, software testing, verification, and validation. Key findings of common weaknesses in the success of projects with large software include the following.

- Long project time lines can impair the ability to forecast future effects of complication due to early decisions.

- Overly stringent, unsubstantiated, or insufficient requirements create significant issues with complexity later in the development cycle. Skills for proper definition and management of requirements are not commonplace.

- Trade studies and system designs must include multidisciplinary technical considerations including software complexity.

- Good software architecture is an important defense against unnecessary complexity, but good software architecting skills are not commonplace.

- Fault management software is among the most difficult to specify, design, and test. Findings include a lack of fault management material in university curricula and the practice of fault logic development separate from control logic, which creates conflicts.

- Exceptionally good software development processes keep defects to near one defect per 10,000 lines of code. Systems that include millions of lines of code will have a significant number of total defects. Software requirement, design, coding, and testing practices are challenged to provide the proper statistical coverage for systems of this scale.

- Embedded systems provide additional challenges to current software engineering practice because of the interplay required between computational and physical constraints of embedded systems. This challenge is not well suited for existing tools (software engineering or otherwise).

- Architecture is about managing complexity. Good architecture—for both software and hardware—provides helpful abstractions and patterns that promote understanding, solve general domain problems, and reduce design defects [1].

Embedded systems design is a challenging composite of system requirements, hardware behavior, and software engineering.

> *We see the main culprit as the lack of rigorous techniques for embedded systems design. At one extreme, computer science research has largely ignored embedded systems, using abstractions that actually remove physical constraints from consideration. At the other, embedded systems*

design goes beyond the traditional expertise of electrical engineers because computation and software are integral parts of embedded systems. [43]

2.2.8 Human Machine Interface

The Human Machine Interface (HMI) functions provide the operator with proper interfaces to guide and direct the control system to operate in the proper modes. The HMI will provide key summary information to the operators in a clear manner. Large systems are prone to large quantities of HMI information such as alarms that must be properly organized and managed. Alarm management is significant task for large hierarchal systems. Flooding operators with large quantities of alarms can limit their ability to understand the most critical alarms and has contributed to problems in facilities such as nuclear plants and refineries [44]. Alarms must be properly classified to their severity and time response requirements to discriminate between long-term maintenance items and critical items demanding immediate attention. Figure 7 illustrates graphically the relationship of alarm categories. As can be seen, as the system moves away from the nominal state space, importance of status indications increases from *alerts* to *alarms*.*

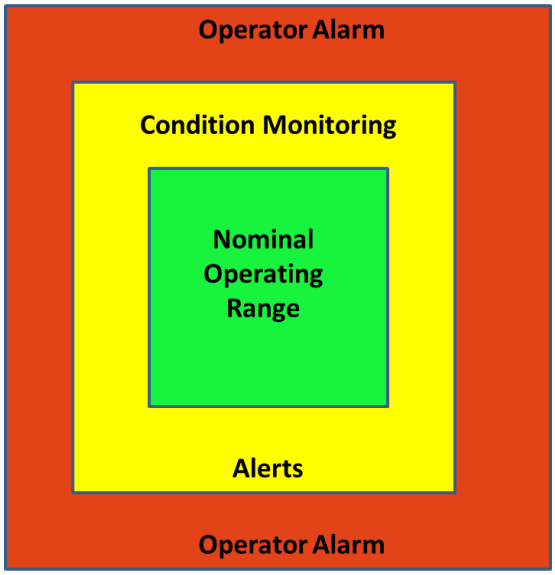


Fig. 7. Graphic description of the relationship of alarm categories. [Adapted from Ref. 44]

2.2.9 Security

The architecture should reasonably facilitate and encourage the five key security countermeasures for industrial control systems [45]..

1 *Security policies*. Security policies should be developed for the control systems network and its individual components, but they should be reviewed periodically to incorporate the current threat environment, system functionality, and required level of security.

* An alert is a notification to be watchful and is not to be considered the same priority as an alarm. An alarm indicates if and when the value (or rate of change value) of a measured or initiating variable is out of limits, has changed from a safe to unsafe condition, and/or has changed from a normal to an abnormal operating state or condition [41].

2 *Blocking access to resources and services*. This technique is generally employed on the network through the use of perimeter devices with access control lists such as firewalls or proxy servers. It can be enabled on the host via host-based firewalls and antivirus software.

3 *Detecting malicious activity*. Detection activities of malicious activity can be networked or host based and usually require regular monitoring of log files by experienced administrators. Intrusion Detection Systems (IDS) are the common means of identifying problems on a network, but can be deployed on individual hosts as well. Auditing and event logs should be enabled on individual hosts when possible.

4 *Mitigating possible attacks*. In many cases, vulnerability may have to be present because removal of the vulnerability may result in an inoperable or inefficient system. Mitigation allows administrators to control access to vulnerability in such a fashion that the vulnerability cannot be exploited. Enabling technical workarounds, establishing filters, or running services and applications with specific configurations can often do this.

5 *Fixing core problems*. The resolution of core security problems almost always requires updating, upgrading, or patching the software vulnerability or removing the vulnerable application. The software hole can reside in any of the three layers (networking, operating system, or application). When available, the mitigation should be provided by the vendor or developer for administrators to apply.

The North American Electric Reliability Corporation (NERC) established the Critical Infrastructure Protection (CIP) standards, which became mandatory in 2008.

1 Identify critical cyber assets
2 Develop security management controls to protect these critical cyber assets
3 Implement personnel risk assessment, training, and security awareness
4 Identify and implement electronic perimeter security for critical cyber assets
5 Implement a physical security program to protect critical cyber assets
6 Protect assets and information within the electronic security perimeter
7 Conduct incident response reporting and response planning
8 Implement recovery plans for critical cyber assets [46].

2.3 INTEGRATION OF REQUIREMENTS-BASED DESIGN AND MODEL-BASED DESIGN PROCESSES

The development of complex engineered systems requires system engineering of many different disciplines such as mechanical, structural, electrical, electronic, software, and human interfaces. Model-driven development or model-based system engineering (MBSE) is one technique to encourage a successful systems engineering outcome [47]. This approach is based on using tools such as Unified Modeling Language (UML) or Systems Modeling Language (SysML) to descriptively model the system behavior, requirements, constraints, and engineered systems such as control systems. UML and SysML are not dependent on a specific methodology or tool; in other words, they can be applied to various methodologies or tool platforms. For example, SysML can describe a software application behavior regardless of the software application language.

The SysML is an open standard modeling language for system engineering applications. It is a tool that supports the specification, analysis, design, verification, and validation of systems. It can describe various processes and systems such as computing hardware, software, data communications, human actions,

operational procedures, and facilities. The SysML is an extension of the subset of the UML, is graphical, and has many implementations [48].

The SysML tool enabled the use of requirement diagrams to efficiently capture functional, performance, and interface requirements [49]. The SysML diagram taxonomy is shown in Fig. 8.

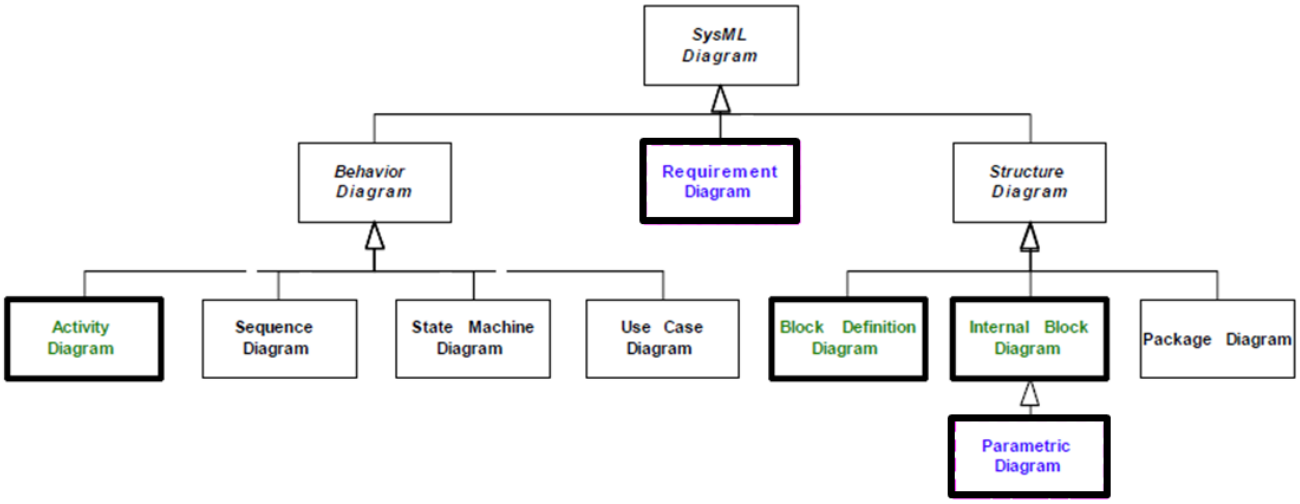


Fig. 8. SysML diagram taxonomy.

As illustrated in Fig. 9, a SysML package includes the following objects and attributes.

1 *Activity Diagram*: Describes the sequence of actions in the process of interest

2 *Block Definition Diagram*: Defines the structure of the system

3 *Internal Block Diagram*: Describes the internal structure of a block

4 *Package Diagram*: Method to group or organize model elements to facilitate larger numbers of model elements

5 *Parametric Diagram*: Describes the constraints among the properties. This integrates behavior and structure models with engineering analysis models.

6 *Requirement Diagram*: Modeling construct for text-based requirements

7 *State Machine Diagram*: Describes the states and state transitions of the desired systems

8 *Sequence Diagram*: Describes the time sequence of a process or action.

9 *Use Case Diagram*: Use cases are independent of the SysML realization of a system. Use cases typically describe the desired operation or outcome of a system. The use case diagram describes the usage of a system (subject) by its actors (environment) to achieve a goal.

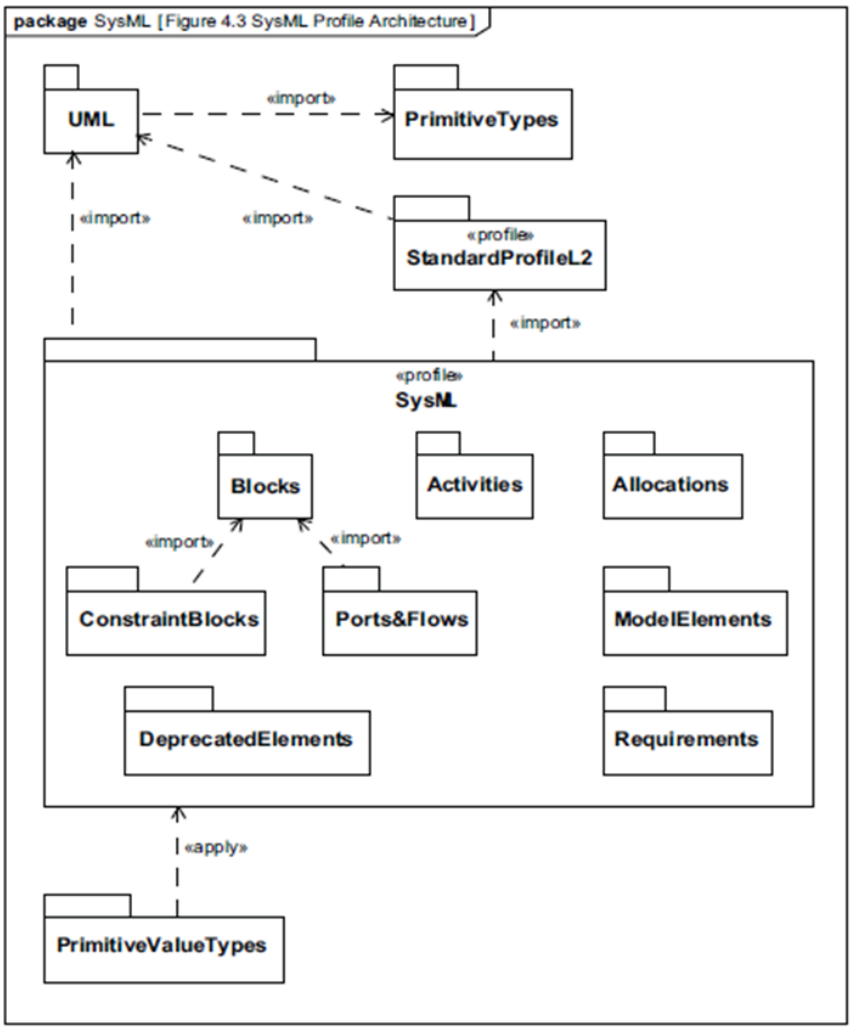


Fig. 9. SysML package structure.

A model-based design process can be applied to mission-critical applications such as the F-35 Joint Strike Fighter [29, 31]. Traditional system engineering practices are described as *document-centric* as they are framed around various documents for requirements, architecture, behavior, and parametrics. Documenting a system using a SysML approach enables a complete system definition of the requirements, architecture, behavior, and parametrics in a single repository or model. This approach offers benefits such as improved requirements traceability, improved analysis of requirement change impacts to the system, ability to reuse models to support updates, and improved early requirements validation [50].

Modeling of process dynamics and control system behavior is an established practice, but the inclusion of requirements, human interaction, operations, procedures, and regulatory considerations is a recent development in system engineering. SysML enables the inclusion of these considerations as shown in Fig. 10. This approach provides insight into many facets of a design including how the design will interact with operations, human operators, and how the design will comply with regulations and requirements for specific use cases or activities.

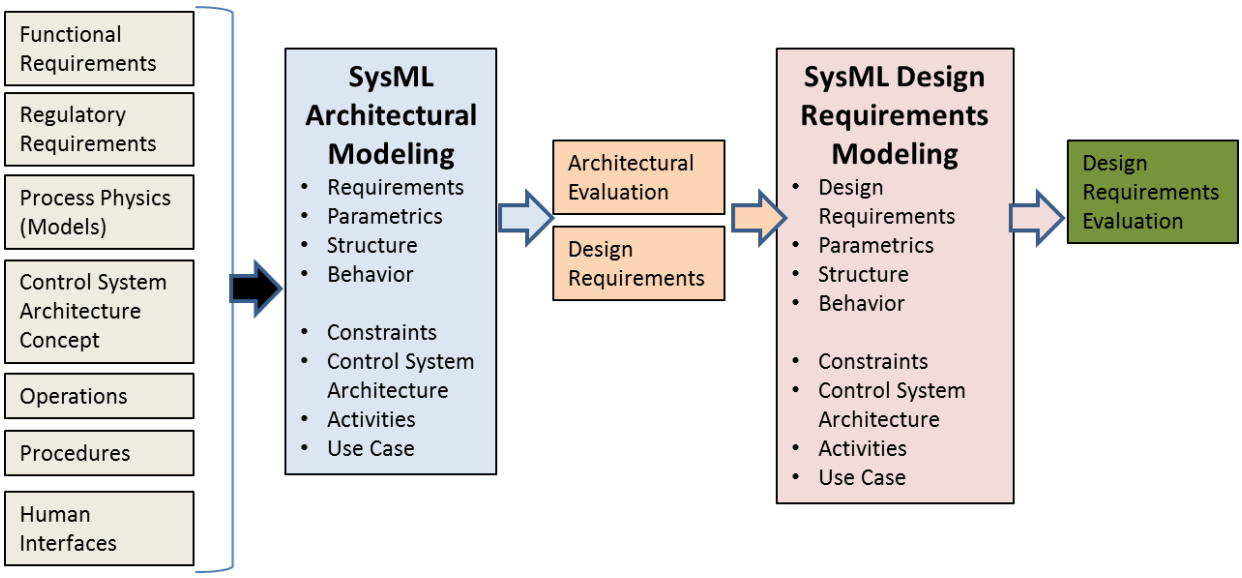


Fig. 10. SysML model-based systems engineering process.

Integrating the capability of SysML and traditional dynamic physics-based modeling tools such as Modelica together in one environment can provide transformative benefits such as requirements traceability, architecture studies, design interdependency sensitivity, reliability analysis, and constraint analysis [51]. This capability can greatly simplify correlating control system performance and stability to system-level operation and requirements. Researchers are developing methods and capabilities to perform this integration. One example is shown in Fig. 11.

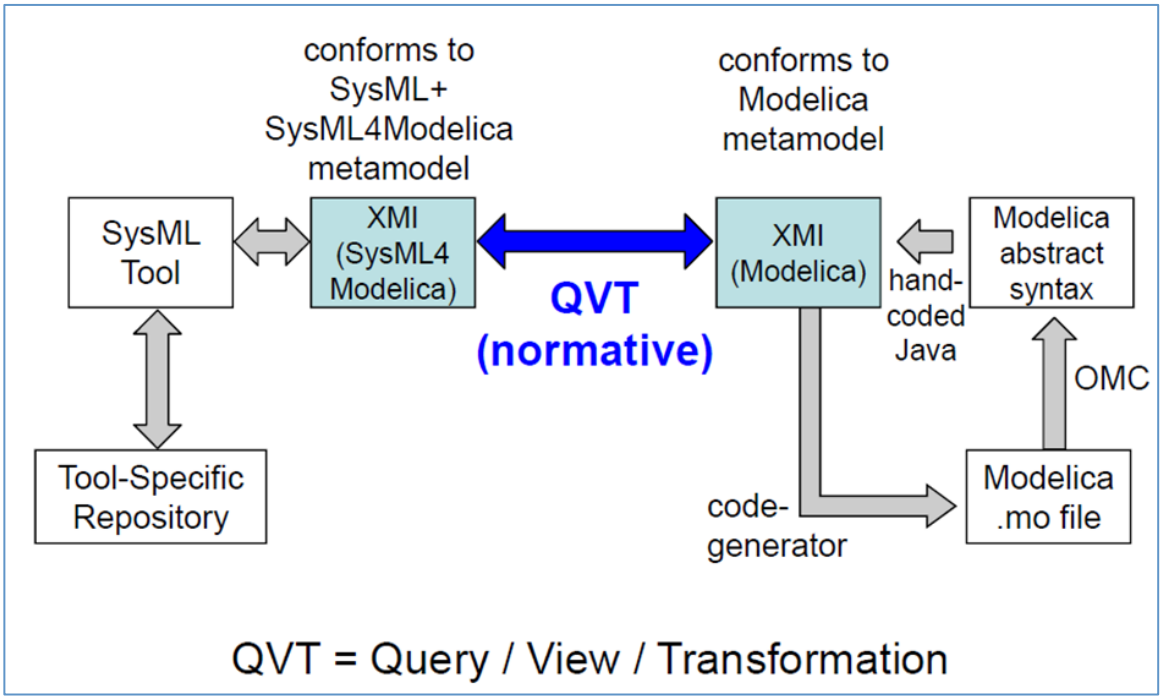


Fig. 11. SysML integration with Modelica. [Ref. 28; used with author's permission]

2.4 SUMMARY—CHAPTER 2

The concepts of systems functionality, performance and stability, environment, communications, reliability, testability, maintainability, human-machine interface, and security were investigated in the context of supervisory control. Modern control systems for mission-critical industries such as aerospace, nuclear, chemical, and defense require multidisciplinary system engineering during all phases of the project. However, the software engineering skills to create robust functional architectures to support high degrees of automation are not commonplace. Architectures, in general, have distinct features that lead to different properties, which then lead to support specific capabilities. The choice of features is often made by following explicit methodological assumptions, driven by the domains and environments for which the design will be implemented.

Early highly automated or autonomous architectures adopted a basic structure designated as *sense-plan-act* (SPA) or *sense-plan-execute* (SPE). In the mid-1980¹s, a layered architecture identified as the *subsumption architecture* was developed for autonomous robots. Numerous robotic and space applications have adopted and expanded the concept. The basic three-layer architecture organizes control algorithms in terms of the functional layer (also called *controller* layer), the coordination layer (also called *sequencer* layer), and the organization layer (also called *deliberator* layer). The layered structure results in successive delegation of duties from higher levels to lower levels; hence, the number of distinct tasks increases as one goes down the hierarchy. Higher levels are concerned with slower aspects of system¹s behavior while responsible for planning with a longer time horizon while the lower levels accomplish real-time action to address the immediate conditions. Based on experience with autonomous applications for robotic and space application, it is clear that the subsumption architecture provides and appropriate basis for the supervisory control system architecture being developed in this research.

2.5 REFERENCES – CHAPTER 2

1 D. Dvorak, *NASA Study on Flight Software Complexity*, NASA Jet Propulsion Laboratory, California Institute of Technology, Report 418878, March 5, 2009.
2 N. J. Nilsson, "Principles of Artificial Intelligence," Palo Alto: Tioga (1980).
3 R. A. Brooks, "A Robust Layered Control System for a Mobile Robot," *IEEE Journal on Robotics and Automation*, v. RA-2, No. 1 (March 1986).
4 J. Connell, "A Colony Architecture for an Artificial Creature," *Technical Report 1151*, Massachusetts Institute of Technology Artificial Intelligence Laboratory (1989).
5 R. Hartley and F. Pipitone, "Experiments with the Subsumption Architecture," *Proceedings of the International Conference on Robotics and Automation* (ICRA) (1991).
6 L. P. Kaelbling, "Goals as Parallel Program Specifications," *Proceedings of AAAI-88* (1988).
7 M. Soldo, "Reactive and Preplanned Control in a Mobile Robot," *Proceedings of the International Conference on Robotics and Automation* (ICRA) (1990).
8 R. C. Arkin, "Integrating Behavioral, Perceptual and World Knowledge in Reactive Navigation," *Robotics and Autonomous Systems*, 6, 105–122 (1990).
9 M. Georgeff and A. Lanskey, "Reactive Reasoning and Planning," *Proceedings of AAAI-87* (1987).
10 R. Simmons, "An Architecture for Coordinating, Planning, Sensing and Action," *Proceedings of the DARPA Workshop on Innovative Approaches to Planning, Scheduling and Control* (1990).
11 J. K. Rosenblatt and D. W. Payton, "A Fine-Grained Alternative to the Subsumption Architecture," *Proceedings of the AAAI Stanford Spring Symposium Series* (1989).
12 D. Payton, J. K. Rosenblatt, D. Kiersey, "Plan-Guided Reaction," *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 20, 1370–1382 (1990).
13 P. Agre, D. Chapman, "What are Plans For?" *Robotics and Autonomous Systems*, Vol. 6, 17–34 (1990).

14 J. Connell, "SSS: A Hybrid Architecture Applied to Robotic Navigation," *Proceedings of the IEEE Conference on Robotics and Automation* (ICRA) (1992).
15 E. Gat, Reliable Goal-Directed Reactive Control for Real-World Autonomous Mobile Robots," Ph.D. Thesis, Virginia Polytechnic Institute and State University, Blacksburg, Virginia (1991).
16 R. P. Bonasso, "Integrating Reaction Plans and Layered Competences Through Synchronous Control," *Proceedings of the International Joint Conference on Artificial Intelligence* (IJCAI) (1991).
17 L. P. Kaelbling, "REX: A Symbolic Language for the Design and Parallel Implementation of Embedded Systems," *Proceedings of the AIAA Conference on Computers in Aerospace* (1987).
18 R. J. Firby, "Adaptive Execution in Dynamic Domains," Technical Report YALEU/CSD/RR#672, Yale University (1989).
19 R. P. Bonasso, et al., "Experiences with an Architecture for Intelligent Reactive Agents," *Journal of Experimental and Theoretical Artificial Intelligence* (June 1992).
20 N. Muscettola, et al., "On-Board Planning for New Millennium Deep Space One Autonomy," *Proceedings of IEEE Aerospace Conference*, Vol. 1, 303–318, Institute of Electrical and Electronics Engineers, Snowmass, Colorado (February 1997).
21 R. Volpe, I. Nesnas, T. Estlin, D. Mutz, R. Petras, H. Das, "The CLARAty Architecture for Robotic Autonomy," *Proceedings of the IEEE Aerospace Conference*, Vol. 1, 121–132, Big Sky, MT, (March 10–17 2001).
22 I. A. D. Nesnas, "CLARAty: A Collaborative Software for Advancing Robotic Technologies," *Proceedings of the NASA Science and Technology Conference*, Adelphi, MD (June 19–21, 2007).
23 P. J. Otaduy, C. R. Brittain, L. A. Rovere, N. B. Gove, "Supervisory Control Concepts for a Power Block with Three Reactors and a Common Turbine-Generator," ORNL-TM-11483, Oak Ridge National Laboratory, Oak Ridge, Tennessee (1990).
24 P. J. Otaduy, C. R. Brittain, L. A. Rovere, N. B. Grove, "Supervisory Control Conceptual Design and Testing in ORNL's Advanced Controls Research Facility," *AI91: Frontiers in Innovative Computing for the Nuclear Industry*, Vol. 1, 170–179, Jackson Hole, Wyoming (September 1991).
25 R. T. Wood, et al., "Autonomous Control for Generation-IV Nuclear Plants," *Proceedings of the 14th Pacific Basin Nuclear Conference*, 517–522, American Nuclear Society, Honolulu
26 E. Gat, "On Three-Layer Architectures," appears in *Artificial Intelligence and Mobile Robots*, D. Kortenkamp, R. P. Bonnasso, R. Murphy, eds., AAAI Press.
27 G. N. Saridis, "Entropy in Control Engineering," *Series in Intelligent Control and Intelligent Automation*, 12, World Scientific (2001).
28 G. N. Saridis, "Hierarchically Intelligent Machines," *Series in Intelligent Control and Intelligent Automation*, 10, World Scientific (2001).
29 J. Clauss, "Implementing the F-35 System Architecture Using UML", Systems and Software Technology Conference, June 18–21, 2007, Tampa Bay, FL, http://sstc-online.org/2007/pdfs/JC1886.pdf
30 Gilvarryh, "IA-32 Features and Flexibility for Next-Generation Industrial Control," *Intel Technology Journal*, 13(1), 146–160 (2009), http://www.intel.com/content/dam/www/public/us/en/documents/technology-Journal/ia-32-next-gen-industrial-control-journal.pdf
31 D. W. Nixon, Flight Control Law Development for the F-35 Joint Strike Fighter, Lockheed-Martin Aeronautics, October 2004, http://www.mathworks.com/aerospace-defense/miadc/presentations/10_F35_Flight_Control_DevelopmentDaveNixon.pdf
32 Wright Laboratory, *Application of Multivariable Control Theory to Aircraft Control Laws*, WL-TR-96-3099, May 1996.
33 Kisner, R., Holcomb, D., Mullens, J., Wilson T., Wood, R., Korsah, K., Muhlheim, M., Qualls, A., Howlader, M., Wetherington, G., Chiaro, P., Loebl, A., "Design Practices for Communications and Workstations in Highly Integrated Control Rooms," NUREG/CR-6991, ORNL/TM-2007/184, September 2009.

34 Information Notice 2007-15, "Effects of Ethernet-Based, Non-safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," US Nuclear Regulatory Commission, NRC Technical Contact Royce Beacom (April 17, 2007).
35 R. Kisner et al., *Design Practices for Communications and Workstations in Highly Integrated Control Rooms*, NUREG/CR-6991, September 2009.
36 T. Fukushima, R. May, and A. Ostenso, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*, Electric Power Research Institute (EPRI), TR-107330, December, 1996.
37 Magnetrol, "Understand Safety Integrity Level," Bulletin: 41-299.4, January 2012.
38 G. Schulmeyer, *Zero Defect Software*, McGraw-Hill, 1990.
39 C. Spitzer, T. Ferrell, and U. Ferrel, RTCA DO-178B/EUROCAE ED 12-B, *The Avionics Handbook*, Chapter 27, http://www.davi.ws/index.php?link=avionics&link2=
40 U.S. Nuclear Regulatory Commission Information Notice 93-57, "Software Problems Involving Digital Control Console Systems at Non-Power Reactors," July 23, 1993.
41 G. Antonelli, "Interconnected Dynamic Systems", *IEEE Control System Magazine*, 33(1), 76–88 (February 2013).
42 D. Morris, "Avionics Operational Flight Program Software Supportability," Wright Research and Development Center Avionics Laboratory, Digital Avionics Systems Conference, Proceedings of 9th IEEE/AIAA/NASA (October 15–18, 1990).
43 T. Henzinger and J. Sifakis, "The Discipline of Embedded Systems Design," *Computer (IEEE)*, pp. 32–40 (Oct. 2007).
44 B. Liptak, *Instrument Engineers' Handbook, Fourth Edition*, *Volume Two: Process Control and Optimization,* Liptak Associates, Stamford, Connecticut, USA, ISBN: 9780849310812, pp. 59–63.
45 US Department of Homeland Security, Control Systems Security Program, *National Cyber Security Division, Recommend Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies* (October 2009). http://ics-cert.us-cert.gov/practices/documents/Defense_in_Depth_Oct09.pdf
46 Energy Sector Control Systems Working Group (ESCSWG), *Roadmap to Secure Energy Delivery Systems*, January 2011.
47 D. Hastbacka, T. Vepsalainen, and S. Kiukka, Model-driven Development of Industrial Process Control Applications, *The Journal of Systems and Software*, 84, 1100–1113 (2011).
48 T. Weilkiens, "System Engineering with SysML/UML," *Modeling, Analysis, and Design*, Elsevier (2006).
49 OMG Systems Modeling Language (OMG SysML), Version 1.3 (June 2012).
50 G. Moser, "Parametric Design and Analysis to Support Model-Based Systems Engineering Using SysML," *NASA Tech Briefs Tech Exchange*, October 1, 2010, http://www.techbriefs.com/component/content/article/8610.
51 C. Paredis et al., "An Overview of the SysML-Modelica Transformation Specification," INCOSE Symposium 2010, Chicago, IL (July 2010).
52 K. L. Shaw, "Wide Range Counting System Digital Upgrade at the High Flux Isotope Reactor," *Transactions of the American Nuclear Society*, Vol. 108, Atlanta, Georgia, June 16–20, 2013.

3. MULTI-MODULE ADVANCED SMALL MODULAR REACTOR REFERENCE PLANT DESCRIPTION

The supervisory control project selected the General Electric Company Power Reactor Inherently Safe Module (PRISM) liquid metal reactor design as the baseline AdvSMR design for demonstration purposes. This conceptual design was originally developed as part of the DOE Advanced Liquid Metal Reactor (ALMR) program. The ALMR PRISM concept consists of reactor modules using a pool-type liquid metal reactor design as shown in Fig. 12. The pool-type design with liquid metal provides unique safety features such as passive shutdown heat removal and passive reactivity shutdown [1].

In this chapter, a brief summary of the ALMR PRISM concept design is presented. More detailed description can be found in Ref. 1. Throughout this report, an advanced reactor is defined as a nuclear reactor that uses a coolant other than water in the primary heat transport system.

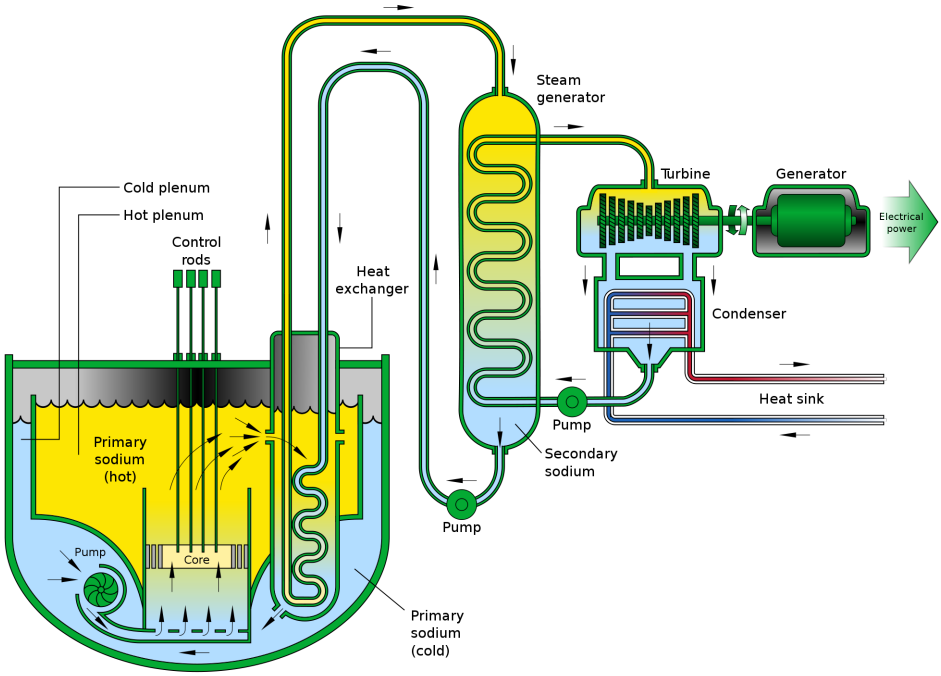


Fig. 12. A schematic drawing for a pool-type sodium fast reactor design.

3.1 OVERALL PLANT DESCRIPTION

The reference ALMR PRISM plant utilizes nine reactor modules arranged in three identical 415-MWe power blocks for an overall plant net electrical rating of 1245 MWe. Each power block features three identical reactor modules, each with its own steam generator that jointly supplies power to a single turbine-generator. Smaller plant sizes of 415 MWe and 930 MWe can be provided by using one or two of the standard power blocks. With incremental power block construction, early revenue can be produced by operating initial power blocks while awaiting completion of subsequent power blocks.

The main power system flow diagram for a standard power block is shown in Fig. 13. Each of the three 425-MW(t) reactor modules has its own steam generator, which is heated by secondary sodium piped from the intermediate heat exchangers in the reactor module. The three steam generators supply 6.66-MPa dry saturated steam to a single power block 415-MW(e) (net output) turbine/generator train.

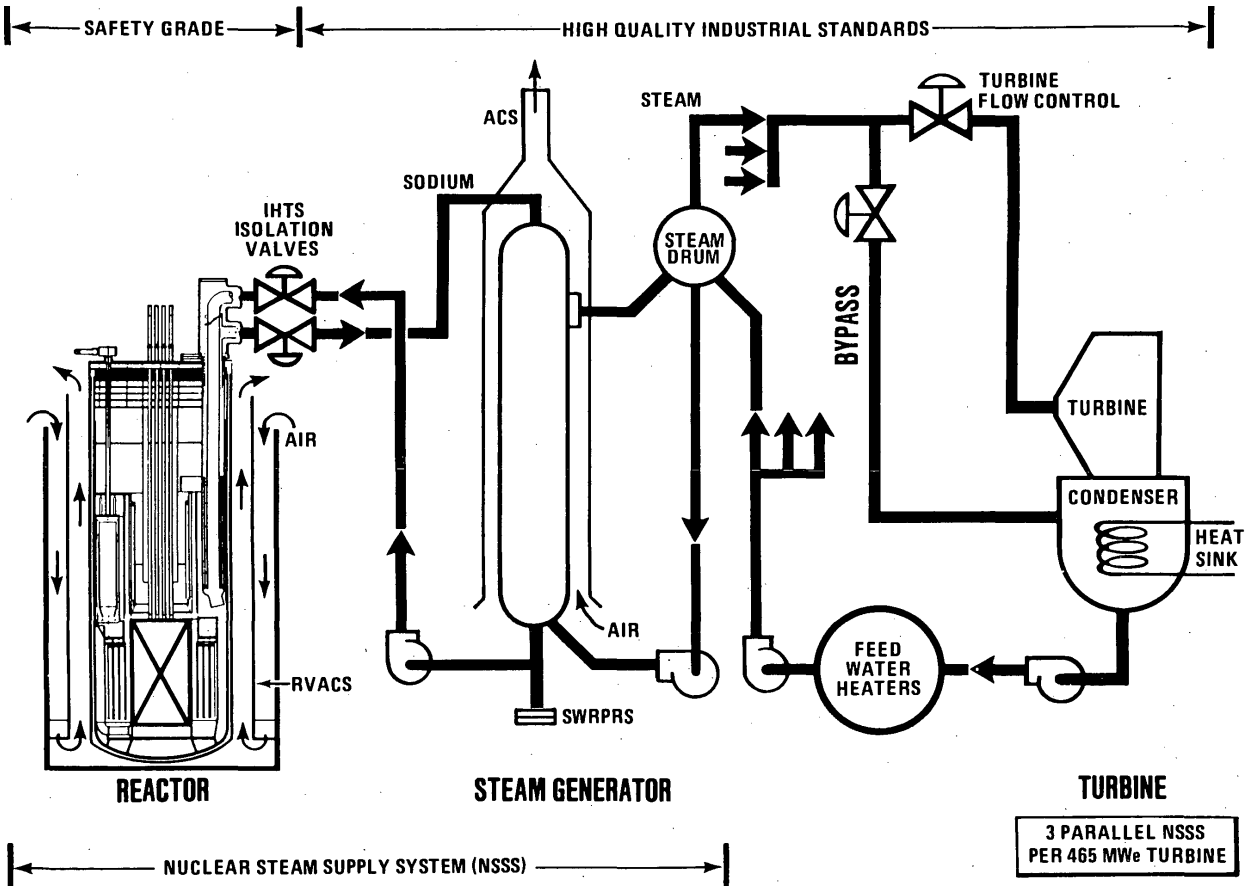


Fig. 13. ALMR PRISM main power system.

The reactor size enables the application of passive, inherent shutdown, and shutdown heat removal features that simplify plant design compared with other concepts. The design combines three reactor and steam-generating modules to form a nuclear steam supply system (NSSS). The NSSS supplies a balance of plant (BOP) with a single turbine/generator train to form a power block for 415-MW(e) output. Nine reactor modules are combined for a 3825-MW(t), 1245-MW(e) power generation plant (Fig. 14).

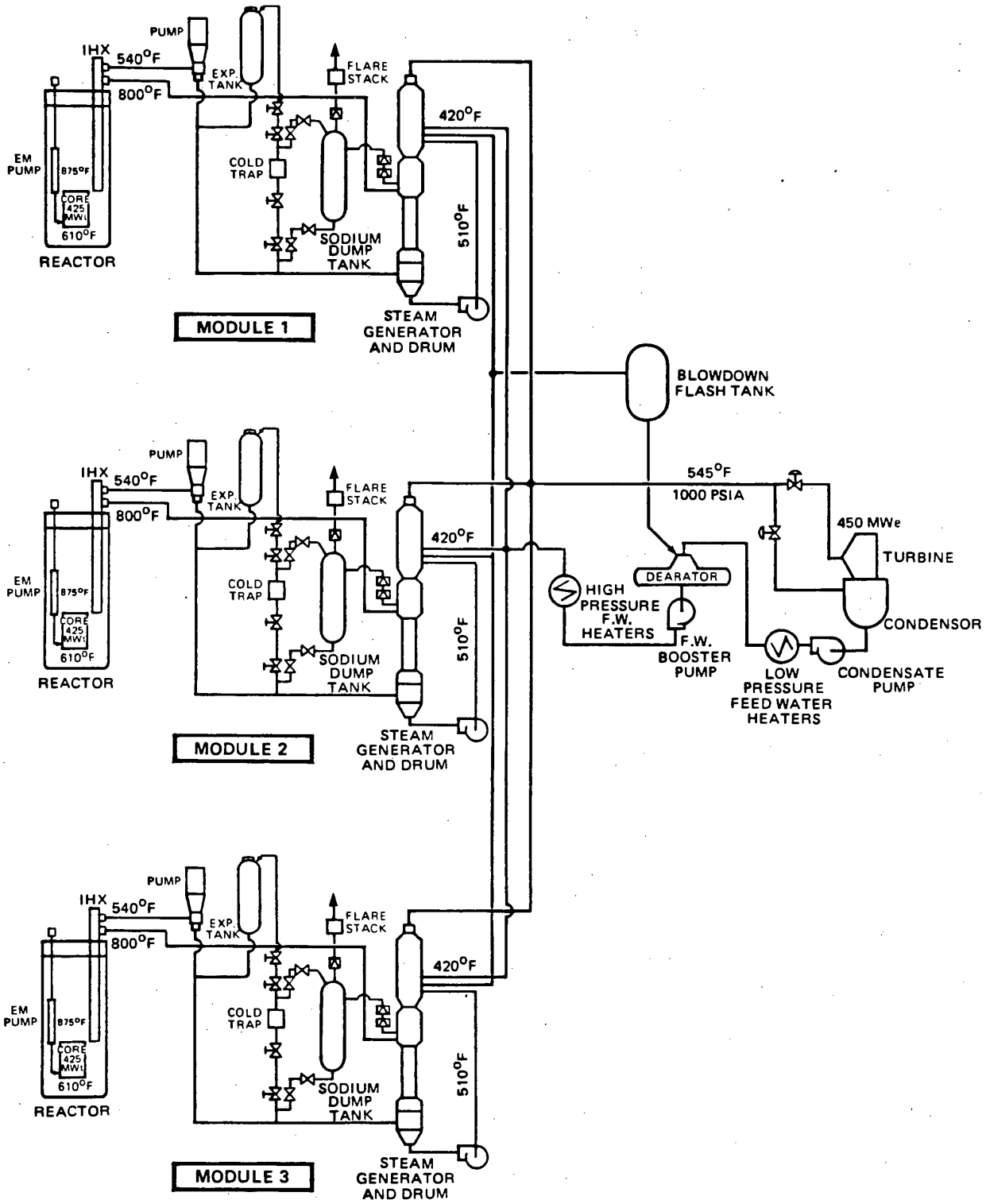


Fig. 14. ALMR PRISM power block heat transport flow diagram.

3.2 REACTOR SYSTEMS

The reactor system consists of the fuel system, the nuclear reaction system, the thermal and hydraulic system, and the active reactivity control and shutdown system. The reactor core is designed to provide a temperature rise of 265ºF with an inlet temperature of 610ºF.

The fuel system generates thermal power through nuclear fission, which is transferred to the liquid sodium in the primary heat transport system (PHTS). The fuel is a uranium-plutonium-zirconium metal alloy. The inherent reactivity control comes from a number of reactivity feedback mechanisms such as Doppler effects and thermal expansion that responds to elevated operating temperature at larger power generation levels. The design operating range is 25% to 100% of rated power.

Reactivity and power are controlled by a system of six control/shutdown assemblies. These provide power and criticality control and can be rapidly inserted to provide a scram shutdown. Two diverse methods for scram are provided: (1) a gravity-driven rod drop and (2) a powered drive system.

3.3 PRIMARY HEAT TRANSPORT SYSTEM

The PHTS provides sodium flow to control the reactor temperature within limits and to transport heat to the intermediate heat transport system.

The PHTS flow path is contained in the reactor vessel. Sodium flows through the reactor core, the hot pool, the shell side of the intermediate heat exchanger (IHX), the cold pool, the EM pump, and the pump discharge piping and the core inlet plenum, as shown in Fig. 15. Each reactor module has two IHXs.

The use of liquid metal sodium as the primary heat transport medium requires the use of specialized pumping systems. Four electromagnetic (EM) pumps are in the reactor module with each pump delivering 0.66 m^3/s with a discharge pressure of 800 MPa. EM pump technology offers a compact size, reduced maintenance requirements, and the absence of mechanical seals and moving parts.

3.4 INTERMEDIATE HEAT TRANSPORT SYSTEM

The intermediate heat transport system (IHTS) transfers heat from the PHTS via non-radioactive sodium flowing through the IHX to the steam generator system. Figure 16 illustrates the IHTS. The IHTS has one loop for each reactor module. The non-radioactive sodium is circulated by a centrifugal pump. An expansion tank allows the IHTS to function as a closed loop system without sodium makeup required due to thermal expansion. The steam generator system provides independent steam generation for each IHTS loop.

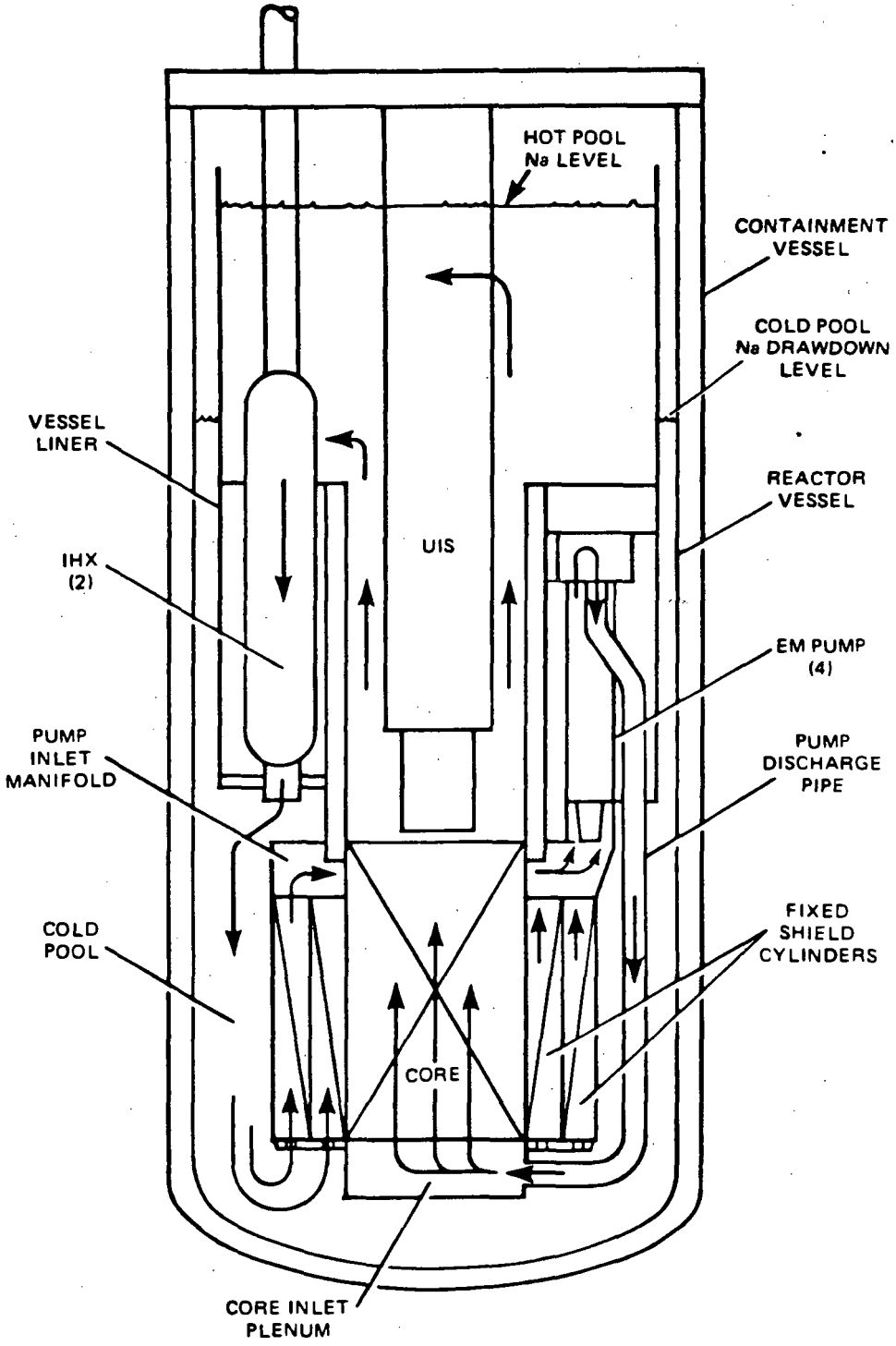


Fig. 15. ALMR PRISM normal sodium flow path in the primary vessel.

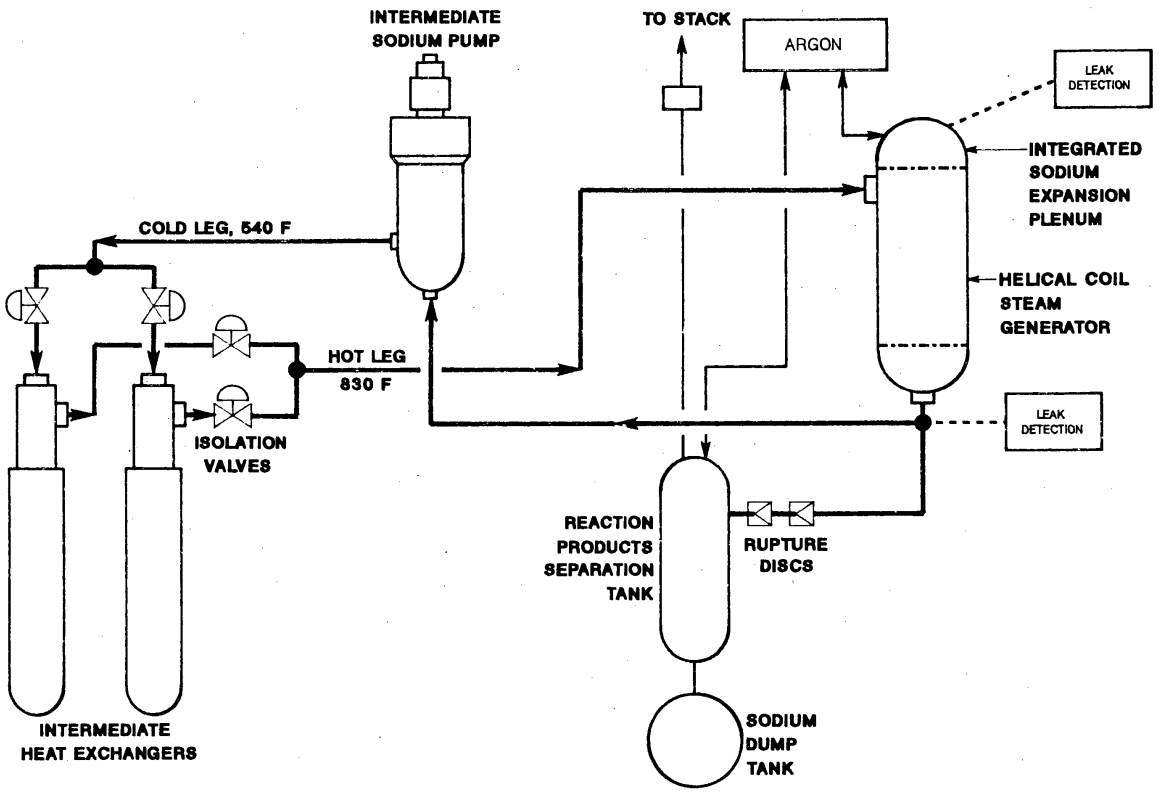


Fig. 16. ALMR PRISM Intermediate Heat Transport System (IHTS) flow diagram.

3.5 POWER CONVERSION SYSTEM

The steam generator is supplied with feedwater, which is partially vaporized by the sodium flowing through the shell side of the steam generator. The saturated water and steam exiting the steam generator is separated to facilitate the steam flowing through dryers and then to the turbine.

The balance of plant dynamics can lead to inter-module oscillations or limit cycle behavior (Fig. 17). The control system for each reactor module could stimulate this undesired behavior. This may become similar to xenon oscillations in a large-core light water reactor (LWR) that requires external action for dampening the oscillations. If one reactor were to provide a different power output versus the other two in the power block and then one or both of the other reactor controls were to reduce their power to provide a constant net power, an oscillation could be stimulated in the balance of plant. The supervisory control system should prevent events of this type and dampen them if they occur. This requirement will be extended to transients such as a reactor scram event.

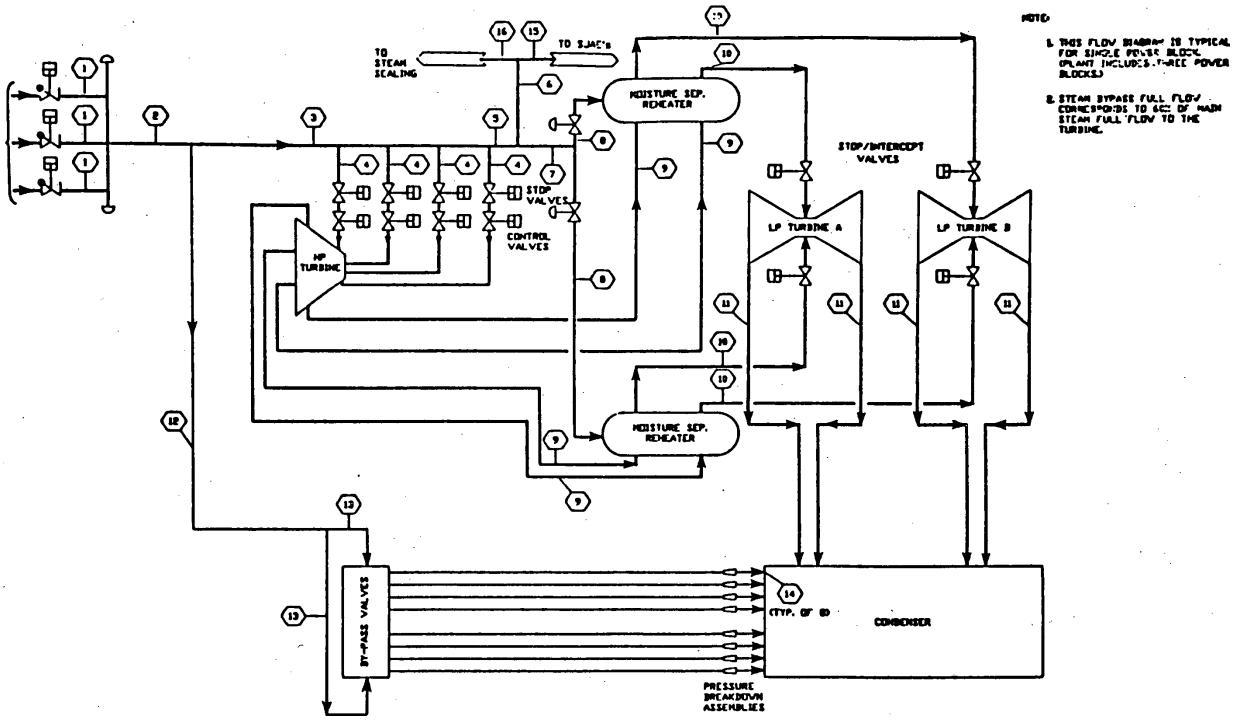


Fig. 17. ALMR PRISM balance of plant main steam and dump system flow diagram.

In a multi-plant nuclear facility, it is likely that each generator would be given independent dispatch signals. It is doubtful that a plant having common turbine generators shared by several nuclear reactors would be adopted unless there is a significant and compelling justification for such a configuration. This conclusion is based on experience at TVA (see Section 2.1.9.1).

3.6 PASSIVE DECAY HEAT REJECTION SYSTEM

The IHTS provides reactor passive decay-heat-removal capability with either a pony motor drive of the centrifugal pump or with natural circulation flow of sodium that will limit reactor temperatures to acceptable values. The combination of negative reactivity feedback, which reduces fission power, and natural circulation for decay heat removal provides inherent passive safety [2, 3].

3.7 INSTRUMENTATION AND CONTROLS SYSTEM

The plant control system (PCS) provides the hardware and software to provide plant control, investment protection, and data management. The PCS is considered a mission-critical system with high-reliability design aspects such as redundant hardware and backup electrical power. The nine nuclear reactor modules, three turbine generators, and the associated balance of plant equipment are controlled from a single control center, as shown in Fig. 18, which is staffed by three reactor engineers and supervised by a shift engineer.

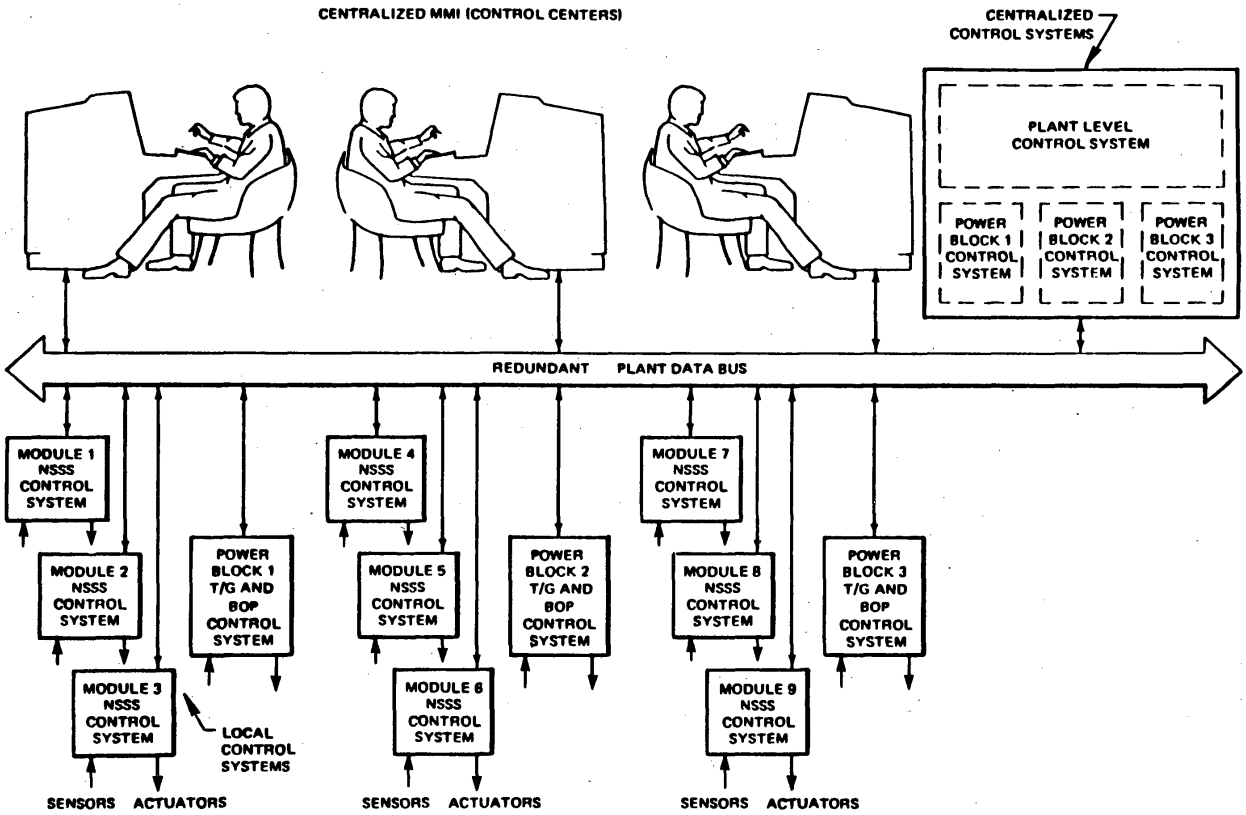


Fig. 18. ALMR PRISM distributed plant control system.

Modern plant automation and man-machine interfaces (MMI) enable the operators to direct all ALMR PRISM control operations efficiently. MMI includes touchscreens, touch panels, and modern consoles. Various information displays, diagnostic programs, and process mimics enable the operators to quickly determine the plant's state and to perform appropriate decision-making. Plant investment protection functions will automatically run back or shut down the reactor to avoid component damage.

The reactor protection system (RPS) uses digital electronics to initiate reactor module safety-related trip functions for the protection of the plant personnel and public safety (Fig. 19). The RPS is classified as a safety system and is independent from the control system. Each of the nine reactors has a local and independent automatic RPS. Trip parameters and trip levels are selected using design basis events (DBEs). Deviations that violate the trip levels will cause the RPS to respond with a reactor trip (scram).

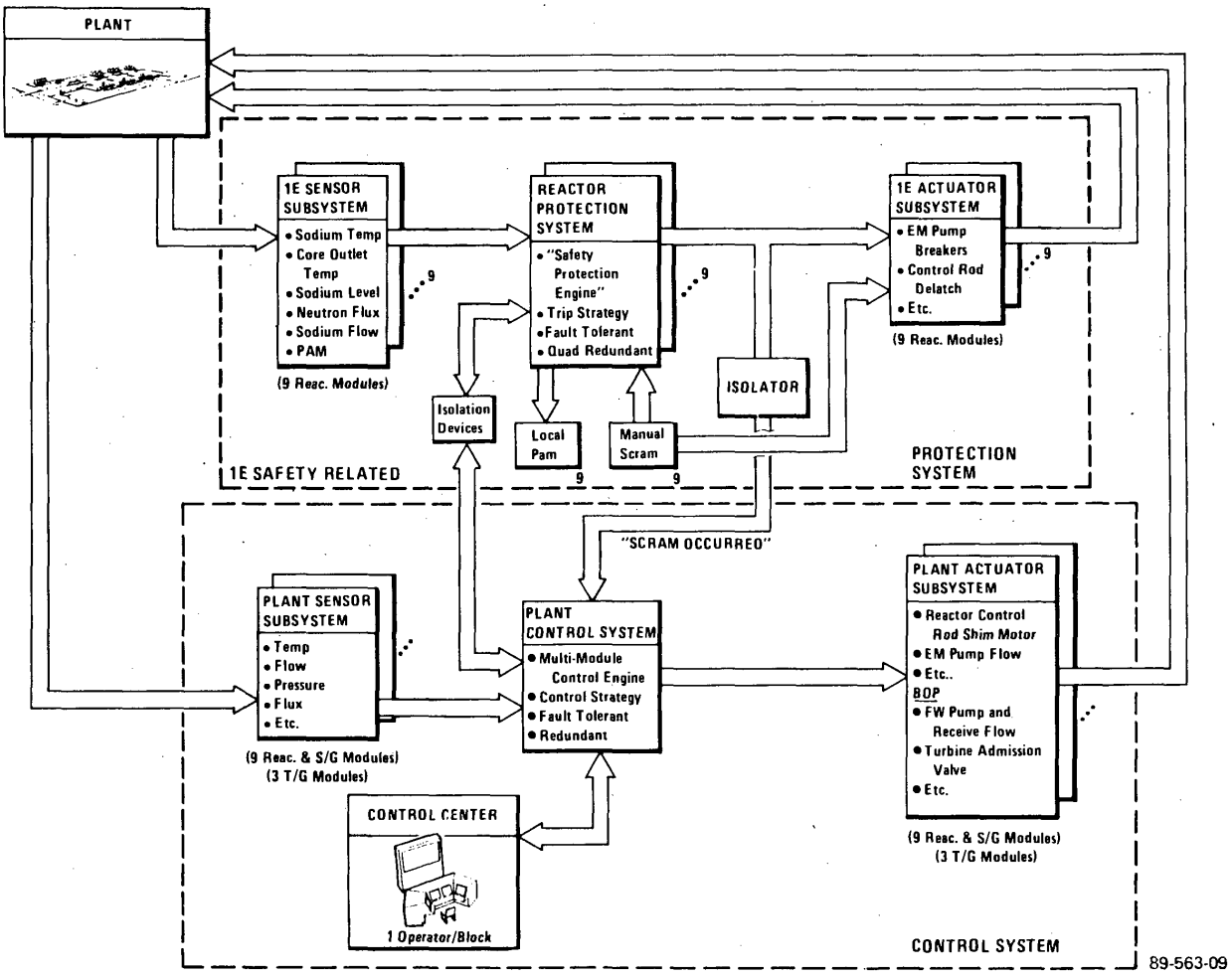


Fig. 19. Plant control and reactor protection system interfaces.

The ALMR PRISM RPS has five reactor trip parameters.

1	*Flux*	Monitor for insertion of reactivity
2	*Flow*	Monitor for loss of flow
3	*Temperature*	Monitor for loss of heat sink
4	*Level*	Monitor for loss of sodium
5	*Pressure*	Monitor for EM pump discharge duct failure

Safety-related instrumentation and control equipment included control building electrical power, control rod safety drive-in motor, coast-down machines for EM pumps, and other mission-critical equipment functions. Safety-related instrumentation consists of reactor vessel instruments that are inputs to the RPS.

The three power blocks, consisting of nine reactor modules and three steam turbine generators, are automatically controlled and automated to a level such that each power block can be controlled by a single operator.

The plant level controller (PLC) automatically supervises and coordinates the balancing of load between the power blocks, and what contribution they make to the total power generation demanded by the grid controller.

The block level controller (BLC) automatically supervises and coordinates each nuclear steam supply system within the power block, and what its contribution to total turbine steam flow will be to meet the demands of the PLC.

3.7.1 ALMR PRISM Control Systems

Digital computer-based systems are applied for automation, reliability, and efficient operation. There are four major levels in the PCS control hierarchy:

- Plant level
- Block level
- System level
- Local (subsystem) level

The PLCs and BLCs are located in the control building. System and subsystem controllers are distributed throughout the plant. The PLC coordinates operation of the three power blocks, and each BLC coordinates its three NSSSs and one BOP system. NSS and BOP controllers in turn coordinate their respective subsystems and local controllers.

The PCS design includes fault-tolerant hardware and redundant communication networks. The plant, block, system, and subsystem control requires real-time, multi-task, and interrupt-driven software features.

3.7.1.1 Data Acquisition and Validation

The PCS observes, monitors, and determines the status of plant components. The data acquisition function gathers data from the various systems and subsystems, validates the data source, records the data, and distributes the data.

3.7.1.2 State Estimator

Some key plant process variables are not directly measureable. The *State Estimator* provides the capability to observe the plant status for variables that are not measured. The State Estimator also validates measurement data.

3.7.1.3 Performance Analyzer

The *Performance Analyzer* function monitors the performance of the plant for startup, shutdown, and energy production. This provides economic metrics and states of the plant related to desired performance goals.

3.7.1.4 Diagnostician

The *Diagnostician* observes plant data and status and contributes to plant control decisions. The Diagnostician provides timely fault identification and anomaly analysis to enable the Control Strategist to select alternate strategies. The value of the Diagnostician is significant during off-normal conditions.

3.7.1.5 Control Strategist

The *Control Strategist* is a significant contributor to coordinating plant control, plant control decisions, and accepting plant direction. The Control Strategist enables meeting requirements such as

- operation of modules and turbines at different power levels,
- sustaining operation through plant maneuvers even with loss of a major component,
- responding to an off-normal service limit event,
- following load demand from the grid dispatcher, and
- allocation of changes in demand and rate of change in energy production and conversion.

The Control Strategist receives information from the operator, *Configuration Manager,* and *Performance Analyzer* and makes decisions regarding the importance of the control objectives and goals. This forms a priority of control decisions and actions. This resolves conflicting goals and objectives and selects the corresponding control strategy based on priority and precedence.

3.7.1.6 Configuration Manager

The *Configuration Manager* applies observed plant status and component availability data to determine appropriate plant configurations to provide acceptable energy production. This feature provides the capability to meet the following requirements:

- sustain operation under loss of a major component,
- respond to trip events, and
- meet reliability goals.

The Configuration Manager is a continuous on-line advisor to the Control Strategist and responds to events with candidate reconfigurations.

3.7.1.7 Maintenance Manager

The maintenance requirements are provided by internal functions described as the *Maintenance Analyzer* and the *Maintenance Planner*. These functions examine the plant status, make maintenance request scheduling decisions, and report plant operation for long-term maintenance. Data from the Diagnostician is used to direct proper short- and long-term maintenance.

3.7.1.8 Control Validator

The *Control Validator* provides a check-before-execute confirmatory step to validate all control commands input by the operator or associated with the selected control strategy. Expected control states are compared with current and target control states. The validation process determines if an operational objective can be reasonably achieved by the selected control strategy and decision. An invalid control command is indicated to the operator to facilitate correction of the command.

3.7.1.9 Command Generator

The *Command Generator* formulates the specific detailed control instructions for the subsystems based on the validated control strategy and commands. The subsystem control commands are also validated.

3.7.1.10 Decision Support

The plant operator has a responsibility in the plant-level decisions. Appropriate information must be provided to the operator to enable proper decision-making. The *Decision Support* function provides the capability to assist the operator in decision-making as an advisor. Based on various information streams from the Performance Analyzer, the Diagnostician, the Maintenance Manager, the Configuration

Manager, and the Control Validator, the Decision Support function performs data fusion and abstraction to provide the operator with clear guidance. This includes

- interpretation and validation of measurements,
- current plant operation status with respect to operational limits, and
- aid to operators in determining the proper priority of decision making.

3.8 SUMMARY—CHAPTER 3

The baseline AdvSMR design selected for development of supervisory control is the ALMR, which is modeled after the General Electric Company ALMR PRISM reactor as documented in the early 1990s. The design utilizes nine reactor modules arranged in block of three. The concept is that a utility can start operation with an initial power block thus generating revenue while awaiting completion of subsequent power blocks. One generator is assigned to each power block. Each reactor in a power block is rated at 425 MW(th). Sodium coolant is used in the primary and intermediate loops. A steam generator is assigned to each reactor. The purpose of supervisory control is to balance power generation from the reactors to electric generation. The original supervisory control system for the ALMR included functional modules to perform data acquisition and validation, state estimation, performance analysis, diagnostics, apply control strategies, equipment configuration management, maintenance management, validate control actions (before execution), and generate command sequences. The basic scheme is similar to that which is under development in the current supervisory control study. Some of the modules have been revised to better function in a Tier-based strategy.

3.9 REFERENCES – CHAPTER 3

1 General Electric, *PRISM Preliminary Safety Information Document*, prepared for the US Department of Energy Under Contract No. DE-AC03-85NE37937 (December 1987).

2 G. Slovik, G. Van Tuyle, and S. Sands, *Assessment of PRISM Responses to Loss of Flow Events*, BNL-NUREG-47818 (December 1992), 019218.

3 G. Van Tuyle, G., Slovik, B. Chan, R. Kennett, H. Cheng, and P. Kroeger, *Summary of Advanced LMR Evaluations – PRISM and SAFR*, NUREG/CR-5364, BNL-NUREG-52197 (November 1989).

4. SUPERVISORY CONTROL SYSTEM ARCHITECTURE DESCRIPTION

Architecture, or more specifically in this context *systems architecture*, is an abstract model that defines structures, components—typically called *entities*—relationships, dynamics, and interactions in a system. An architecture description is a formal description and representation, organized in a way that supports reasoning about structures of the system, composed of system components, externally visible properties of these components, interfaces, relationships and interactions between them.

Architecture provides a method to describe complex systems in terms of abstract entities, which can be used to represent multiple components in a system that share *common attributes*. In other words, it describes what the elements of a system are and imposes high-level *rules* that describe how these elements connect and interact with each other in way to deliver the mission of the system. The architectural rules are constraints that restrict the design to conform to certain standards, which typically lead to common *topography*.

Common attributes require that components or subsystems of a system be represented in an abstract manner that describes its functions in terms of underlying physical phenomena. For instance, a thermocouple is a device that measures the temperature of a medium. However, what it essentially accomplishes is to convert temperature differentials to electrical current, which is ultimately registered by an electrical indicator. So, in an abstract manner, it *transduces* a physical property into an electrical signal. Therefore, it belongs to the *sensor* class.

The key objective of the supervisory control system is to reduce cognitive load on reactor operators by taking on routine operator actions executed primarily during normal operations, and some actions performed during startup and shutdown. The supervisory control system is not to replace the operator as the key decision node for safety-related actions, nor is it to support or complement protective actions performed by reactor protection or engineered safety feature's actuation systems.

From the systems perspective, the role of the operator in the control room is to generate and execute control actions as the primary decision block in the sense-command-execute feedback loop. An abstraction of the flow of information is represented in Fig. 20. The role of the operator is represented within the transparent box: operator is to continuously update decisions based on his or her perception as a result of the cognitive analysis. Operators may also perform some information analysis based on direct readings of sensory data and develop high-level commands.

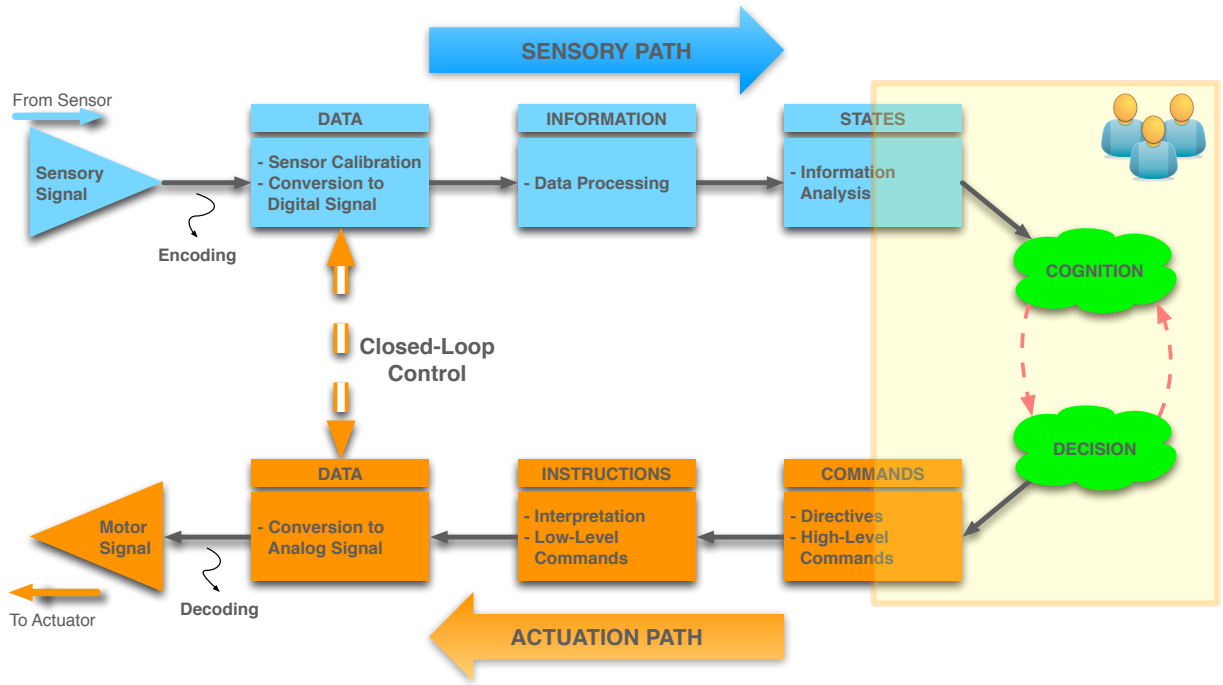


Fig. 20. Flow of information in a sense-command-execute loop.

The supervisory controller presented in this context automatically performs a portion of the cognition/decision processes as well as information analyses and command generation based on a consistent, predefined rule set, which essentially provides a mapping between the monitored plant variables and plant status information, and acceptable actions at any given time. The set of actions as function of plant variables and status can be constructed using the rules defined in plant-specific technical specifications.

4.1 DEGREES OF AUTOMATION

Autonomous control systems are intended to perform well under significant uncertainties in the system and environment for extended periods of time. These features are typically built in these control systems to improve system resilience and increase overall system availability.

Table 1 suggests a scale of *degrees of automation* proposed by Sheridan [1]. Each new level, which increases the automation of the control system, provides opportunities for machine error while precluding human intervention. The question to be answered is

> *"What is the appropriate level of automation for an advanced SMR?"*

This scale is not an absolute quantitative grading. Though it is a subjective scale, it still represents a logical attempt to define the space of autonomy in a finite number of levels. However, since the extreme cases—that is, no autonomy and full autonomy—are fixed, the decomposition is consistent as it follows a monotonically increasing level of self-control.

The exact degree of autonomy is a design decision. However, for a nuclear plant control system, we expect that the degree of automation will be between 4 and 7 on this scale.

Table 1. Scale of degrees of automation [1]

Level of Autonomy	Anticipated Control Function
1	The computer offers no assistance, operators must do it all
2	The computer offers a complete set of action alternatives, and
3	narrows the selection down to a few, or
4	suggests one, and
5	executes that suggestion if the operator approves, or
6	allows the operator a restricted time to veto before automatic execution, or
7	executes automatically, then necessarily informs the operator, or
8	informs the operator after execution only if the operator asks, or
9	informs the operator after execution if it, the computer, decides to
10	The computer decides everything and acts autonomously, ignoring the operator

Two classes of system control were originally proposed by Kisner and Raju [2]: continuous and discontinuous. To many, the distinction between discontinuous-event control and continuous-event control is unclear because in past designs role allocation assumed that human operators perform most of discontinuous activities (e.g., start-stop and valve lineup) and local (continuous) controllers regulate to maintain a setpoint. To automate a large-scale system, both classes of control must be integrated to carry out the functions required to achieve the goals and objectives of the entire plant.

Subsystems that exhibit continuous parameter variation—and thus may be controlled by proportional control·—fall under the first category of continuous control. The second category, discontinuous control, refers to subsystems that exhibit discrete operational states and are called on to function by an enabling command with no element of proportionality contained in the command.

An example of the interaction between continuous and discrete control is shown in Fig. 21. In the diagram, an initiation (external to the system) moves the system state from *I* (a shutdown state) to *J* by enabling operation of the controller for subsystem A and starting a device related to that subsystem. The initiating condition could also have transmitted set points to subsystem A as well as other commands and parameters. In the example, outputs from the controlled subsystems also become initiating conditions for transitions to new states ultimately moving to state *K* (a normal operating state). An external initiation of condition 4 begins the transition eventually back to the shutdown state *I*.

· Proportional control is a type of control in which the amount of corrective action is proportional to the amount of error, as in a controller in which an error signal—that is, the difference between measured output and reference input—is amplified by a constant gain to form a controller output.

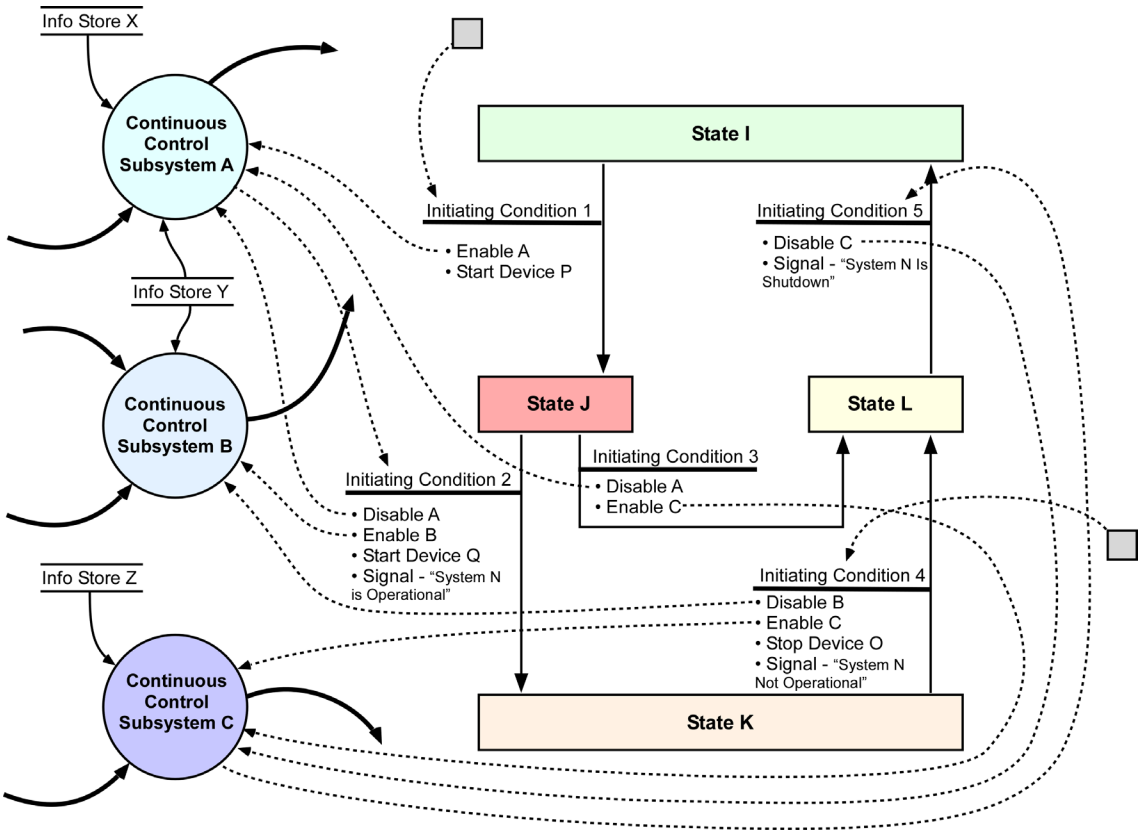


Fig. 21. Illustrative example of interaction between discrete state control and continuous control.

4.2 FUNCTIONAL ELEMENTS OF DECISION MAKING

The key safety feature is that operators have ultimate supervisory override control of autonomy functions. Furthermore, autonomous actuations should be highly visible and transparent to plant operators.

In order to achieve the desired level of autonomy, the control system must possess certain design features such as fault detection and isolation and decision-making. The following sections briefly discuss these features.

As illustrated in Fig. 22, decision-making is a recursive process involving many tasks that continuously feed each other in order to converge into a single strategy or action [3]. To achieve a representative decision-making attribute, the supervisory control system should contain the proper functional elements.

Fig. 22. Elements of decision-making process.

The following sections briefly define the necessary elements to accomplish decision-making and strategy development. These modules are still in development; therefore, exact functions might evolve as the project continues.

4.2.1 Planning and Scheduling Module

The *Planning and Scheduling Module* (PSM) is responsible for long-term planning and scheduling tasks. The module takes dispatch inputs and operator requests and creates a series of operation plans and action schedules with a desired time horizon. These plans and schedules are dynamically evaluated with reasonable frequency and take into account the overall condition of plant systems and major components as well as the life-cycle economic cost of each plan.

The PSM is the main module that implements the cost-minimization functions. There might be a number of them, which are intended to maximize plant availability with a hard constraint of minimizing critical asset downtime. This constraint, in fact, should increase overall plant availability over the plant life cycle.

The PSM module is hierarchically at the organization layer and is implemented in software.

4.2.2 Data Acquisition Module

The *Data Acquisition Module* (DAQ) reads sensor data from plant sensors, including sensors in Tier-I, -II and -III systems. The DAQM is also responsible for executing necessary validation routines to verify the credibility of sensor data. Validation methods might include cross validation, consistency with plant trends, and model-based calculations.

The DAQM converts the raw sensor data to a consistent digital value that is used across the plant. During the conversion process, various filtering techniques may be employed depending on the sensor transduction method and signal noise content.

The DAQM is hierarchically in the functional layer and contains both hardware and software elements.

4.2.3 Plant Status Analysis Module

The *Plant Status Analysis Module* (PSAM) interprets raw sensor data collected from plant sensors. Depending the on the sensor reading, the data is filtered and checked against other similar sensor reading using cross-correlation methods. Faulty readings are identified and communicated to the *Decision Making Module* (DMM), which flags the information as potentially inaccurate, to modify subsequent decision strategies accordingly.

The PSAM hierarchically sits in the organization layer, and is implemented in software.

4.2.4 Diagnostics and Prognostics Module

The *Diagnostics and Prognostics Module* (DAPM) is responsible for monitoring and assessing the health status of critical components in major plant systems. Hierarchically, it belongs to the coordination layer as it directly interfaces with the Tier-II sensors.

The on-line monitoring (OLM) signals can be used for (1) early detection of anomalies in a component—*diagnostics*—and (2) estimation of remaining useful life—*prognostics*. The supervisory control design utilizes these tools to make decisions for operation of the plant.

Diagnostics and prognostics information is a critical capability in achieving and improving the level of autonomy in a system. The diagnostic system continuously monitors critical components using all available sensor data. The data is then used to identify signatures that point to departure from nominal operating conditions.

The majority of diagnostic data is provided by Tier-II sensors as they are specifically added for this functionality. However, Tier-I sensor data may also contain useful information, which can be combined with Tier-II sensor data to create a more complete status of a component.

Research under a DOE Nuclear Energy Research Initiative (NERI) project included efforts to establish the basis for on-line fault detection and isolation (FDI) of sensors and field devices in a nuclear power plant. A prototypic FDI system includes the following capabilities:

- rule-based decision making,
- fault isolation using fault residuals and pattern classification,
- steady-state and transient operational conditions—measured or simulated, and
- combinations of sensors and actuators.

Figure 23 illustrates the FDI approach for on-line monitoring. The isolation of device faults is performed using both rule-based decision-making and pattern classification of prediction error vectors in the fault space. This integrated approach enhances the fault diagnostics capability and provides a robust method for FDI. The rule-based expert system uses the system behavior characteristics for each fault based on measured or simulated data. Applications have employed data-driven models to characterize sub-system dynamics and subspace identification using the singular value decomposition technique. Residual generators are designed using the dynamic parity space approach to be sensitive to all faults but one so

that they can support isolation of particular faults. For most of the cases, the system dynamic behavior responds differently for each component fault.

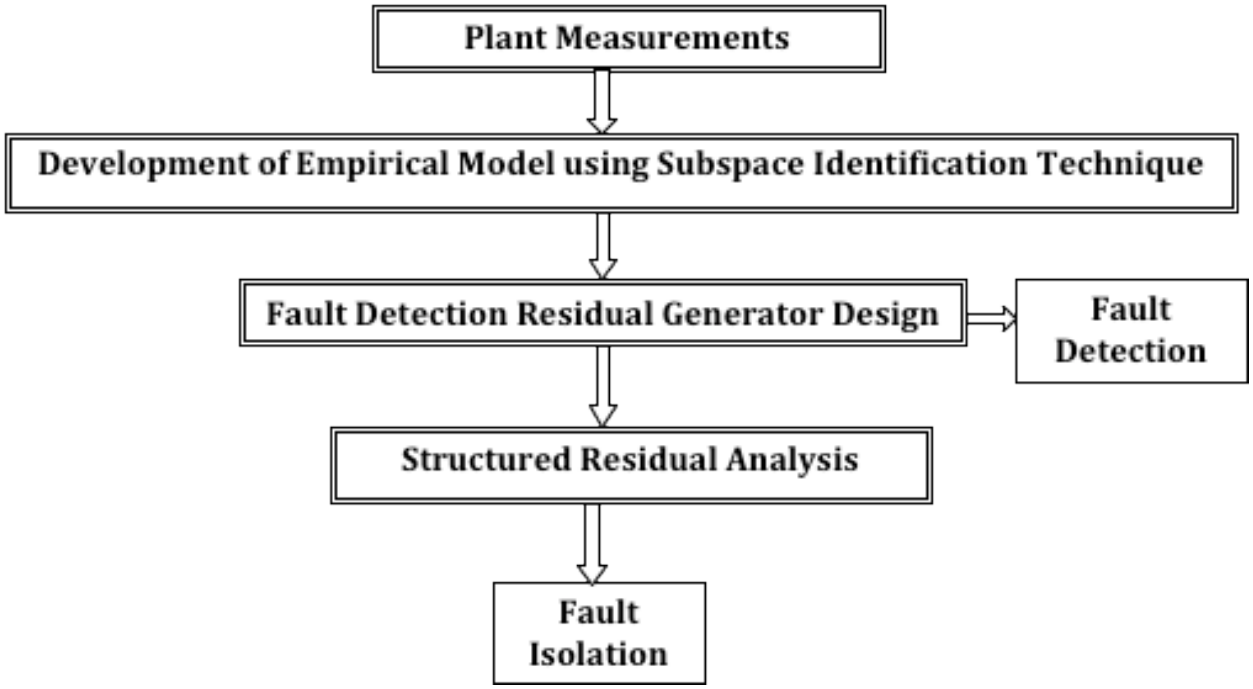


Fig. 23. Approach to on-line fault detection and isolation monitoring.

These FDI techniques have been successfully applied to a laboratory process control loop, a simulated U-tube steam generator, and a simulated helical-coil once-through steam generator. In addition to successful detection and isolation of dual faults, the approach has been shown to be robust in the presence of measurement noise and operational transients.

The DPM module is implemented in software.

4.2.5 Decision Making Module

Decision-making is defined as a process that generates a resulting *decision*—or in more general terms a direction in action based on some bounded set of rationality. Every decision-making process produces a final choice. The output of the decision-making process is generally an instruction, which will be executed to be turned into an action. Figure 24 illustrates the decision-making process at a functional level [3].

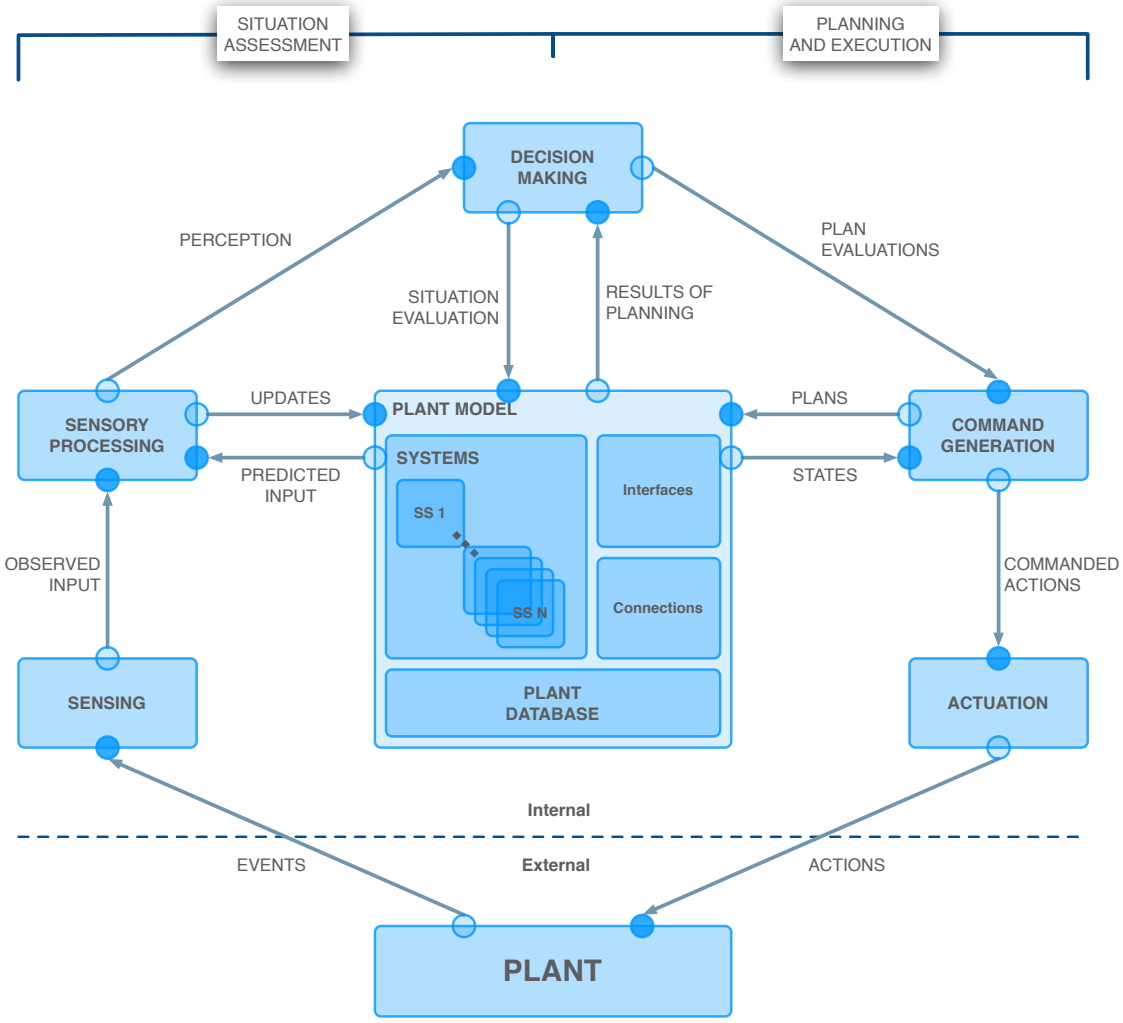


Fig. 24. Functional relationship between modules in decision-making process.

The *Decision Making Module* (DMM) is the master agent in supervisory control hierarchy. As illustrated in Fig. 25, it gets plant status information from the *Plant Status Analysis Module* (PSA), and the current schedule matrix from the *Planning and Scheduling Module* (PAS). It also accepts and prioritizes operator inputs and dispatch requests. Diagnostic evaluations and prognostics assessments are included in the information provided by the PSA module.

The DMM has the highest authority in the hierarchy. It is implemented in software.

4.2.6 Control Action Prediction and Validation Module

The *Control Action Prediction and Validation Module* (CAPV) runs a sufficiently high-fidelity end-to-end systems model of the plant with accurate interfaces. It accepts inputs from the DMM and the PSAM modules to execute the instructions. If the simulation indicates a potential risk or instability, the forwarded action is flagged and communicated to the DMM, which in turn may eliminate the control action—depending on the plant status.

The CAPVM is hierarchically in the organization layer and is implemented in software.

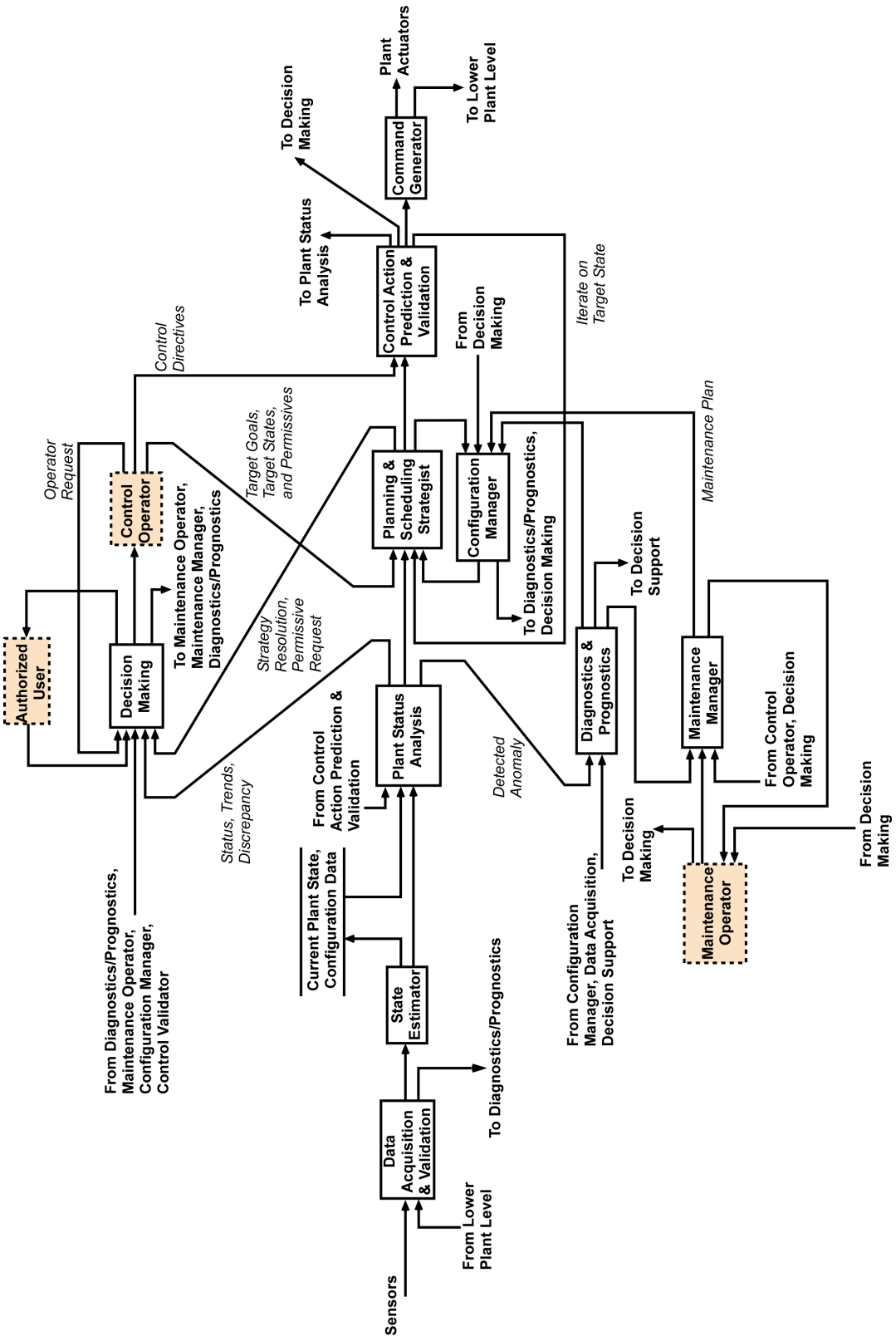


Fig. 25. ALMR PRISM conceptual generic control engine model.

4.2.7 Command Generation Module

The *Command Generation Module* (CGM) is a translation element in the coordination layer that links the organization layer to the functional layer. The CGM module translates the instructions from the DMM module—after being verified by the CAPV module—into proper hardware signals.

The CGM is implemented in hardware and software.

4.3 METRICS FOR ARCHITECTURE

For the supervisory control architecture, the project team primarily investigated two quantitative analysis options: (1) probabilistic risk assessment (PRA)–based analysis, and (2) analysis based on informatics entropy.

The PRA-based analysis options will be discussed in this section, while the entropy-based approach will be introduced in Chapter 6, "Information Theoretic Approach to Architecture."

4.3.1 PRA-Based Analysis

This section offers two potential applications of PRA tools: (1) off-line optimization during design phase and (2) real-time optimization and decision-making.

4.3.1.1 Optimization during Design Phase

Reliability is a measure of the likelihood that the system has not experienced any failures. In evaluating any design, both qualitative and quantitative reliability analyses can provide insights into the reliability, fault tolerance, diversity, and redundancy of alternative design options. Because of the importance of the supervisory control system, it is vital to select the best system for the job.

Fault-tolerant designs are important for digital-based systems. Automatic recovery and reconfiguration mechanisms play a crucial role in implementing fault tolerance because an uncovered fault may lead to a system failure even when adequate redundancy exists [4].

Redundancy alone does not guarantee fault tolerance. The only thing redundancy guarantees is a higher fault arrival rate compared to a simplex system of the same functionality. For a redundant system to continue correct operation in the presence of a fault, the redundancy must be properly managed [5]. Redundancy management issues are deeply interrelated and determine not only the ultimate system reliability but also the performance penalty paid for fault tolerance.

Defense-in-depth is used to ensure the system cannot fail unless multiple components fail to perform their design functions. Because the supervisory control system for the AdvSMRs will require multiple, independent failures to occur for the system to fail, system failure will be dominated by dependent failure scenarios.

The next step in the development of the system architecture will be incorporating what has been learned performing this task with specific specifications on control functions on a system-by-system basis and hardware/software architecture alternatives. Insights on fault protection methods will aid in designing a reliable supervisory control system.

Four methods of fault protection are used to achieve a high reliability for systems:

1 design and implementation standards where the reliability of every constituent component is as high as reasonably achievable,

2 system-level modular redundancy with functionally equivalent elements executing identical tasks in parallel where results of individual redundant subsystems can be evaluated against a majority to prevent propagation of individual subsystem errors from control operations,

3 design diversity of duplicate but independently developed functions to guard against generic design errors in an I&C controller of duplex or N-modular designs, and

4 added hardware and/or software for fault detection and recovery where self-testing is constantly monitoring for generic hardware or software failures and signaling redundant subsystems or supervisory systems to reset and restart failed functions or to logically reconfigure the control system around the failed subsystem.

Software can also be used to implement fault tolerance against hardware faults by

1 fault detection, such as the software voting on results of replicated processors;
2 fault isolation, where the software executes self-testing programs;
3 repair by switching off the failed subsystem; and
4 recovery by reinitializing a failed task.

4.3.1.2 Use of PRA Tools for Assessment of I&C Architecture Options

PRA-based analyses will be useful—and necessary—to optimize the design of the supervisory control system. There are many system layouts that can meet the fault tolerance criteria for the supervisory control system. The difficulty is in choosing the right one. The fault tolerance methods described above will help in choosing the right one.

The supervisory control system for the AdvSMRs must successfully integrate all of the necessary sensors and actuators, their signal processing electronics, and the transmission of data between transducers and the control computers. Primary sensors included are typically temperature (T), flux (F), and pressure (P) sensors. Process computers analyze the sensor data and if actions are required, transmit a signal to the control rod drives, EM pumps, and/or valves.

Some examples of fault-tolerant architectures are discussed below [6]. These examples show that there are numerous fault-tolerant architectures available for consideration that will require further study to prioritize the design options.

The simplest reactor controller (RC) design, as shown in Fig. 26, uses identical redundant sensors, RCs, hardware, and software. Redundant channel sensors relay a signal to a redundant signal conditioner (SC). Any of the three channel sensor outputs (P, T, or F) is sufficient for reactor control. Thus, all three sensors or the channel SC must fail for reactor control from an RC to be unavailable. Independent sensor inputs to each RC guarantee different input values to each RC because of sensitivity and calibration differences between the sensors and SCs. As sensor faults develop, isolating the failed sensor is essentially impossible because no comparative calculations between redundant channels are performed.

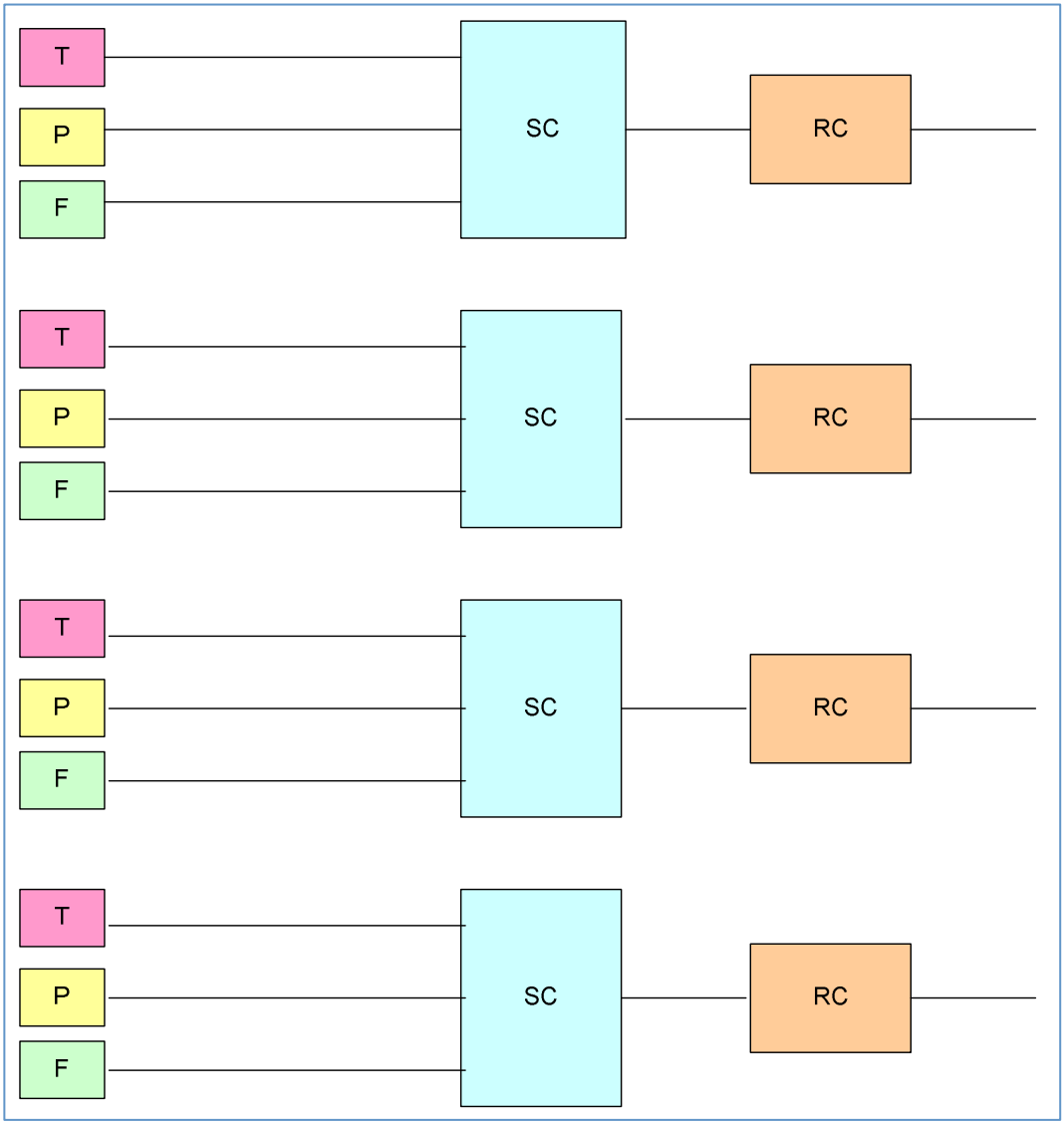


Fig. 26. Independent sensor inputs and control outputs. [T, P and F are sensors; SC is a signal conditioner, and RC is reactor controller]

Two types of enhancements over the simplex system include

1. modular redundant controllers, sensors, actuators, and communications; and
2. diverse controllers, sensors, actuators, and communications.

Sharing independent sensor values to all four RC channels should produce identical control calculations, as illustrated in Fig. 27. An identical algorithm calculates a consensus value in all four RC channels. Unlike the simplex design in Fig. 27, when a sensor fails, a common deviation-checking algorithm should isolate the sensor fault. Even if all three sensors to a particular SC fail, the corresponding RC should still be available to calculate consensus input values from shared sensor inputs from redundant channels. Penalties for being able to share sensor data include added mass and wiring complexity for point-to-point sensor value sharing. Software complexity also increases because of the ability to calculate consensus input value and to check input deviation.

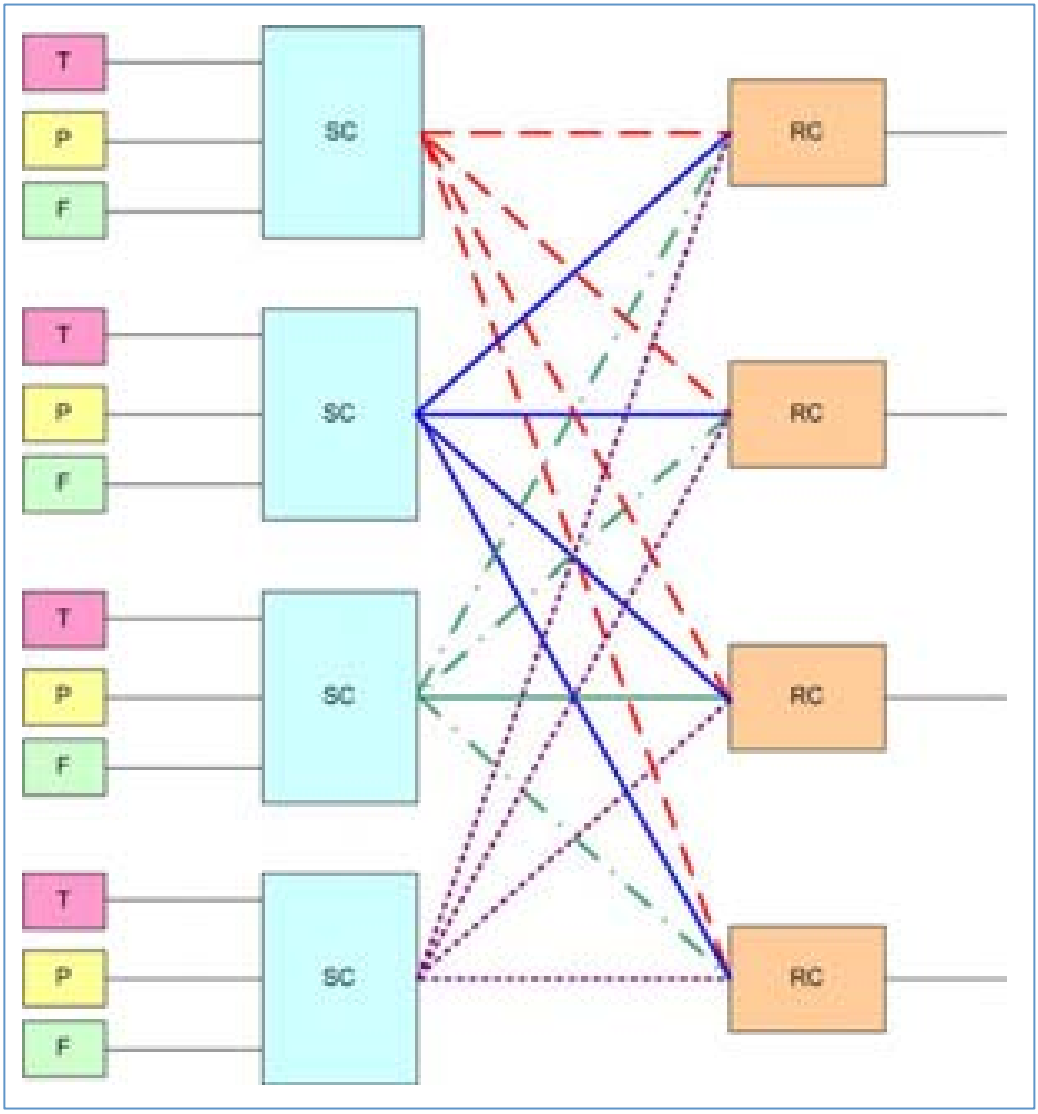


Fig. 27. Independent sensor inputs shared between independent controllers.

In this example, PRA-based methods were successfully used to demonstrate fault tolerance of an I&C architecture for a given set of mission objectives.

4.3.1.3 Real-Time Optimization and Decision Making During Operations

The controllable day-to-day costs of AdvSMRs are expected to be dominated by operation and maintenance costs. Health and condition assessment coupled with online risk monitors can potentially enhance affordability of AdvSMRs through optimized operational planning and maintenance scheduling. Currently deployed risk monitors are an extension of probabilistic risk assessment (PRA). Currently, most nuclear power plants have a PRA that reflects the as-operated, as-modified plant; this model is updated periodically, typically once a year. Risk monitors expand on PRA by incorporating changes in the day-by-day plant operation and configuration (e.g., changes in equipment availability, operating regime, environmental conditions). The development of a framework for enhanced risk monitors (ERM) being developed by Pacific Northwest National Laboratory (PNNL) would enable accurate characterization of the real-time risk during operation and maintenance activities [7].

Risk-informed operations management will most likely be the most important aspect of the supervisory control strategy in maximizing the plant availability. This risk management and decision module of the supervisory control systems makes extensive use of diagnostics and prognostics calculations of critical structures, systems and components (SSCs), which have implications for plant operations and maintenance activities. Condition and status of these critical assets are taken into account in developing operations strategies (i.e., long-term scheduling) or modifying existing strategies for maximum electricity generation, and steam (or an alternate fluid medium) delivery to the process heat plant over a long time window.

The supervisory control system can increase system reliability and plant availability by using ERMs to capture real-time characterization of plant status.

4.3.2 Information-Theoretic Approach: Entropy

The information-theoretic approach to system organization and control system design has recently gained traction and appears to be a promising method for analysis of complex system structures and interactions.

This topic is discussed in detail in Chapter 6, "Information Theoretic Approach to Architecture."

4.4 HIERARCHICAL STRUCTURE OF THE SUPERVISORY CONTROL ARCHITECTURE

In the first milestone report on supervisory control, we discussed the commonly accepted structure of hierarchy for control at modern chemical plants, as briefly recapped here.

From the functional point of view, the hierarchical structure of state-of-the-art control implementations indicates that layering of control strategies based on the time constants of actuation results from pure evolutionary process of practical engineering needs. In modern chemical processing plants, model predictive controllers (MPC) are a component in a multi-level hierarchy of control functions. Figure 28 illustrates a hypothetical plant having a conventional control structure (Unit 1, left) and a model predictive control structure (Unit 2, right). The supervisory level determines optimal steady-state settings for each unit in the plant over daily time horizons. The settings are sent to local optimizers that run more frequently and may have more detailed models of the unit under control. The dynamic-constraint control implements local optimizer outputs by moving the plant between constrained steady-state conditions while minimizing constraint violations en route.

In the conventional structure of Unit 1, the control implementation is accomplished using combinations of PID algorithms, Lead-Lag compensation, and High/Low select logic. At this level, translation of the control requirements into an appropriate conventional control structure is difficult—every process is unique; there is no standard structure. For Unit 2, the combination of blocks at the dynamic-constraint control level is replaced by a single MPC controller. MPC accomplishes feedback controller synthesis by (1) measuring the current control process state then (2) rapidly computing the next state for the open-loop control function. The first portion of this function is used during a short time interval, after which a new measurement of the function is computed for a new measurement. The measure and computer process is continually repeated the procedure. Though born out of the efforts of practical process control engineering, this predictive construct has spawned much research in the controls community.

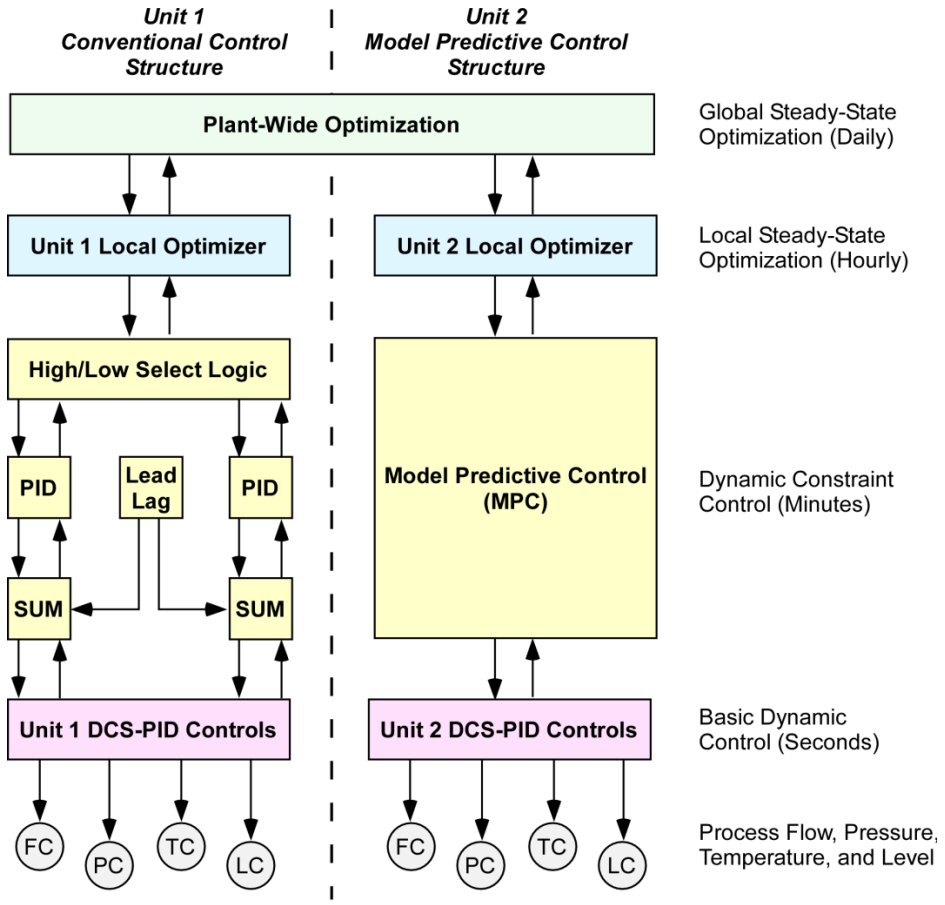


Fig. 28. Comparison of conventional and model-predictive control functions in a typical chemical plant.

An important point can be made that dynamic control must be embedded in the hierarchy of plant control functions in order to be effective. Four levels of control can be described that correlate with the structure in Fig. 29.

Level 3: Time and space production scheduling
Level 2: Setpoint optimization to minimize cost and ensure production quality and quantity
Level 1: Dynamic multivariable plant control
Level 0: Ancillary systems control; PID control of valves

In relation to the proposed supervisory control architecture, Level 0 and Level 1 belong to the functional layer, whereas Level 2 and Level 3 correspond to the coordination layer and the organization layer, respectively.

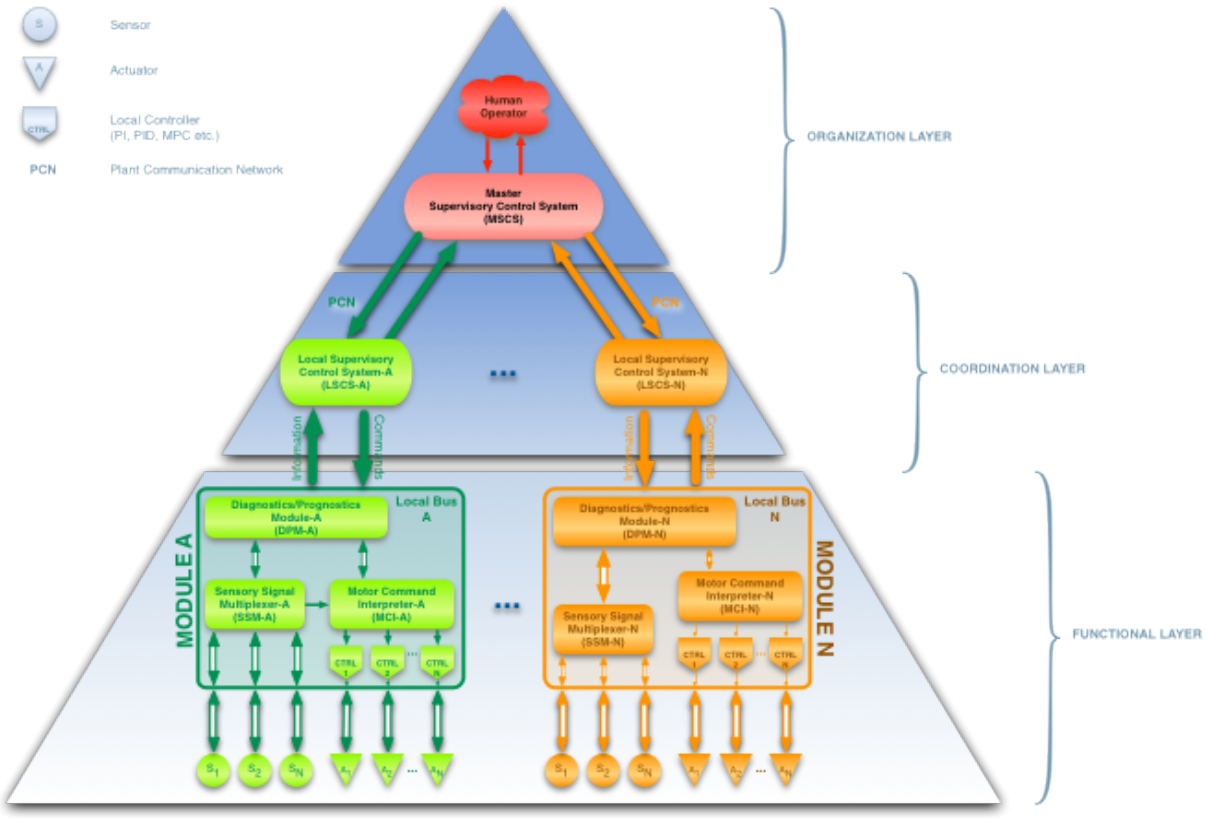


Fig. 29. Supervisory control system architectural topology showing sensing and actuation interfaces.

The supervisory control at the organization layer (layer 1) provides control for the power blocks in the coordination layer (layer 2) and the reactor modules in the functional layer (layer 3). Stand-alone units at multi-unit sites commonly share Tier II (support) and Tier III (utility) systems. However, because of the increased sharing of systems between reactor modules (see Appendix A), some Tier I (heat removal) systems may be shared at AdvSMRs. This introduces new management and control criteria at Layer 1 and Layer 2 of the supervisory control system.

4.4.1 Functional Layer

The functional layer includes hardware and software elements responsible for performing the tasks in the direction of the instructions generated by the coordination layer.

4.4.2 Coordination Layer

Coordination layer is an intermediate layer that essentially performs two functions.

1. Process and interpret low-level plant data acquired from a large network of plant sensory inputs (i.e., convert data to information), and relay this information to the organization layer consistent with the language of the decision modules.

2. Process high-level directives generated by the decision modules in the organization layer and convert them to *unique* instructions to be performed by the modules in the execution layer.

4.4.3 Organization Layer

Organization layer is the master supervision module that is responsible for decision-making, validation, and planning and scheduling.

4.4.4 Rules That Govern Interactions between Layers

Typically, in three-layer architectures, interactions are allowed only between adjacent layers, that is, between the coordination layer and the functional layer, and the organization layer and the coordination layer.

This architectural constraint that restricts data or instruction exchange between all modules is a manifestation of variations in processing capabilities in individual layers as well as a result of interfaces.

Nominally, the functional layer provides raw sensor data to the coordination layer and executes the low-level instructions given by the coordination in response to the directions by the organization layer.

4.5 INTERFACE REQUIREMENTS FOR SUPERVISORY CONTROL ARCHITECTURE

Interface requirements are typically component specific, and in certain cases the requirement may be at a subsystem level. From the architecture point of view, there are three distinct interface requirements for the supervisory control:

1. feedback control loop interface requirements,
2. diagnostics and prognostics module interface requirements, and
3. supervisory control interface requirements

4.5.1 Functional Layer Interface Requirements

Functional layer is comprised of a large number of local loop control elements. Closed-loop control is typically the preferred method for continuous regulation of processes. It can be as simple as *proportional* (P), *proportional-integral* (PI), or *proportional-integral-derivative* (PID) controllers, or may employ model-based control techniques that rely on optimizing a preferred cost function.

Feedback control is a powerful method, which relies on base correction actions on the difference between desired and actual performance signal, such as an output value. The use of feedback resulted in vast improvements in system stability, controllability, and performance. An example block diagram of a PID controller is shown in Fig. 30.

Loop control may also include feedforward elements, which are typically used to improve disturbance rejection capability of a system. Feedforward control is particularly useful in shaping the response to command signals because command signals are always available. Since feedforward attempts to match two signals, it requires good process models; otherwise the corrections may have the wrong amplitude or phase. For certain dynamics, it is advantageous to combine feedback and feedforward controls.

In a typical loop control, two interfaces are required: sensing and actuation. The loop control provides a tight coupling between the sensors and actuators.

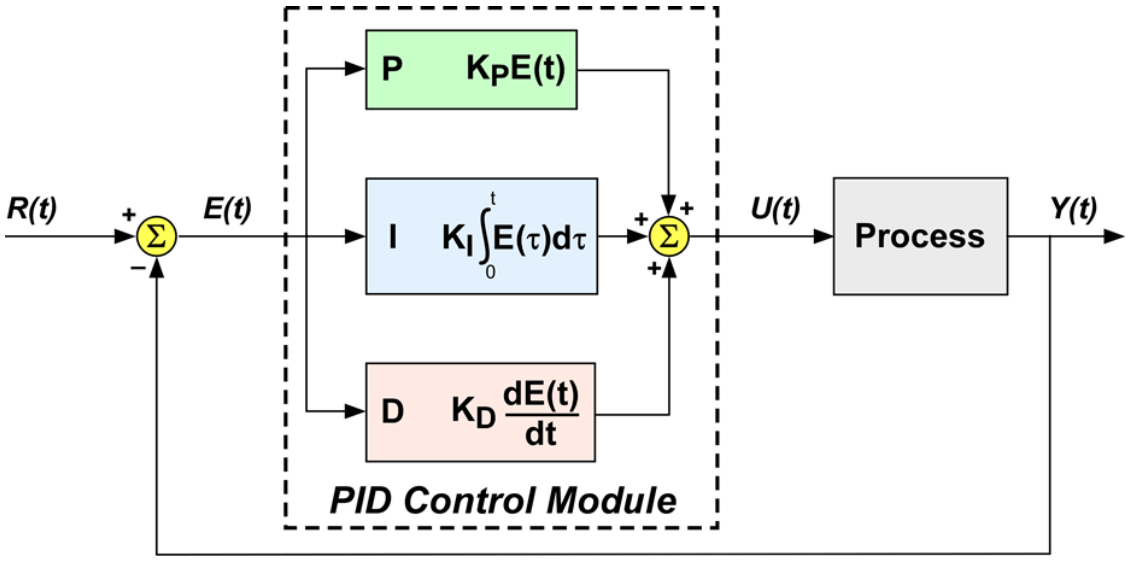


Fig. 30. Block diagram of a PID controller in a feedback loop.

4.5.1.1 Sensing Requirements

Sensing requirements for a loop controller depend on the controller design. For single-input single-output (SISO) systems with P, PI, or PID controllers, the only sensing requirement is the plant output signal, $y(t)$. The error signal, $e(t)$, is obtained by the difference between the *setpoint*, $r(t)$, and the plant output signal, that is,

$$e(t) = r(t) - y(t).$$

Multiple-input multiple-output (MIMO) systems perform tracking and regulation of more than one signal. This is also the case for control system designs that rely on model-based controls, such as model-predictive control (MPC). For MPC, in order to meet the stability requirements, the system is required to be observable, which means that a minimum number of state variables must be measured for the closed-loop system to be controllable.

If the sensor dynamic introduces significant phase to the measured signal—potentially due to a large time constant—it might be reasonable to incorporate the sensor dynamics into the plant model. Measurement of temperature by a thermowell in fast fluid flow is a good example to sensor dynamic with a relatively large time constant.

4.5.1.2 Actuation Requirements

For SISO systems, the actuation signal, $u(t)$, which is the input signal, is calculated using the error signal, $e(t)$, with the following mathematical relationship:

$$u(t) = \underbrace{K_p e(t)}_{\text{proportional}} + \underbrace{K_i \int_0^t e(\tau)d\tau}_{\text{integral}} + \underbrace{K_d \frac{de(t)}{dt}}_{\text{derivative}},$$

where K_p, K_i and K_d are called proportional, integral, and derivative gains, respectively.

Similarly, for MIMO control systems and model-based control systems, there might be more than one actuation paths.

Actuator dynamics may also become important, particularly for actuators that rely on mechanical elements, for example, hydraulic, pneumatic, moving or rotating components. If the response of these components introduces significant time delay—also called *time lag*—actuator dynamics should also be incorporated into the plant dynamics.

4.5.2 Coordination Layer Interface Requirements

Coordination layer is the mediating layer between the organization layer and the functional layer. Sensing requirements of the coordination layer arise from one of its functional modules: diagnostics and prognostics module.

4.5.2.1 Sensing Requirements

Diagnostics and prognostics technologies—also called *on-line monitoring*—have become increasingly more popular. Especially with the advances in digital technology, it is possible to include significant computational power in relatively small form factors at rates as high as real time.

Diagnostics and prognostics modules may be used for continuous monitoring of components of interest. A salient example in a nuclear power plant is loose-parts monitoring in the primary boundary and in steam generators. In conventional nuclear power plants, this is typically provided to control room operators as additional information.

There are a large number of methods for diagnostics. Though some of these techniques rely on the relationship between input and output signals, having additional sensory data for critical parts of a component may deliver important information about its health status, in addition to the signature analysis. For instance, for mechanical components with moving and rotating parts operating at high speed, accelerometers provide useful information about the vibration status of certain structures. Deviations from a baseline during normal operating conditions may indicate a structural problem.

Sensor arrangements on a component for on-line monitoring can be made arbitrarily high. However, cost may become prohibitive for complex components, particularly for those in harsh environments. Therefore, assessment of sensing requirements is a trade-off between the amount of necessary data and sufficient information for reliable diagnostic capability.

Prognostic modules provide information about the future condition of a system or component. A typical performance indicator is *remaining useful life* (RUL).

4.5.2.2 Actuation Requirements

Coordination layer interfaces with Tier-II actuation devices. Proper limits, checks, and permissives will be developed in the subsequent phases of the project to avoid spurious actuations.

4.5.3 Organization Layer Interface Requirements

Organization layer is responsible for decision-making, planning, and scheduling. Therefore it has no sensing or actuation interfaces that would allow it to acquire raw data directly or send actuation signals.

Organization layer has a *language* that is composed of a limited number of instructions, which are to be decoded by the coordination layer. The decoded instructions are transferred to the functional layer.

4.6 INTERLOCKS AND PERMISSIVES

Plant safety systems such as the Reactor Protection Systems (RPS) or the Engineered Safety Features Actuation System (ESFAS) have priority over the supervisory control system functions. Hence, once the RPS or the ESFAS actuate, the supervisory control system is not allowed to override any safety-related function or take actions that would counteract or impede the effectiveness of such functions.

These requirements and rules can be implemented using the safety-related *interlocks* that would eliminate certain functionalities of the supervisory control system. However, this is a design decision. Safety-related interlocks are part of the plant safety systems and, hence, are regulated.

Permissives can be used to implement special provisions to enable certain supervisory control functions in helping perform auxiliary *post-event* cooling functions. It should be noted again that this is a design decision. Since it relates to some level of interaction with plant safety systems, extensive FMEA or Failure Mode, Effects, and Criticality Analysis (FMECA) as well as PRA analyses must be performed to ensure that safety system functionality is not compromised.

4.7 SYSTEM-LEVEL FUNCTIONAL TAXONOMY

System-level functional taxonomy is an essential step to create interface descriptions for the supervisory control system.

The primary purpose of major plant systems in a nuclear power plant, or in any power generation system, is to transfer heat through the necessary components to finally deliver it to the turbine/generator trains and to the ultimate heat sink, as illustrated in Fig. 31. In typical temperature ranges of operation, about one-third of the generated heat is converted to electrical power, while close to two-thirds of the heat is dumped to the environment. For reactor outlet temperatures, a higher fraction of the heat is converted to electrical power, leading to higher thermodynamic efficiency.

In our approach to creating an architecture for the supervisory control system, we propose that the plant systems be broken down into three tiers based on their functions:

1. Tier-I systems,
2. Tier-II systems, and
3. Tier-III systems.

The technical basis for a three-tiered decomposition is mainly for logical and practical reasons: the first tier is considered to be directly involved in this high-level goal of transferring heat from the source to the sink. Naturally, systems in this tier provide direct interfaces for sensing the status of heat flow, and proper means for actuation to deliver stabilizing actions. This can be clearly seen in Fig. 31: The systems in this tier have only a limited number of sensing and actuation channels. For instance, for the ALMR PRISM plant, the number of control variables per reactor module and the power conversion system is limited to six. These are represented as the following demand signals:

1. Reactor power demand,
2. Primary heat transport system flow demand,
3. Intermediate heat transport system flow demand,
4. Recirculation flow demand,
5. Feedwater flow demand, and
6. Turbine load/steam flow demand.

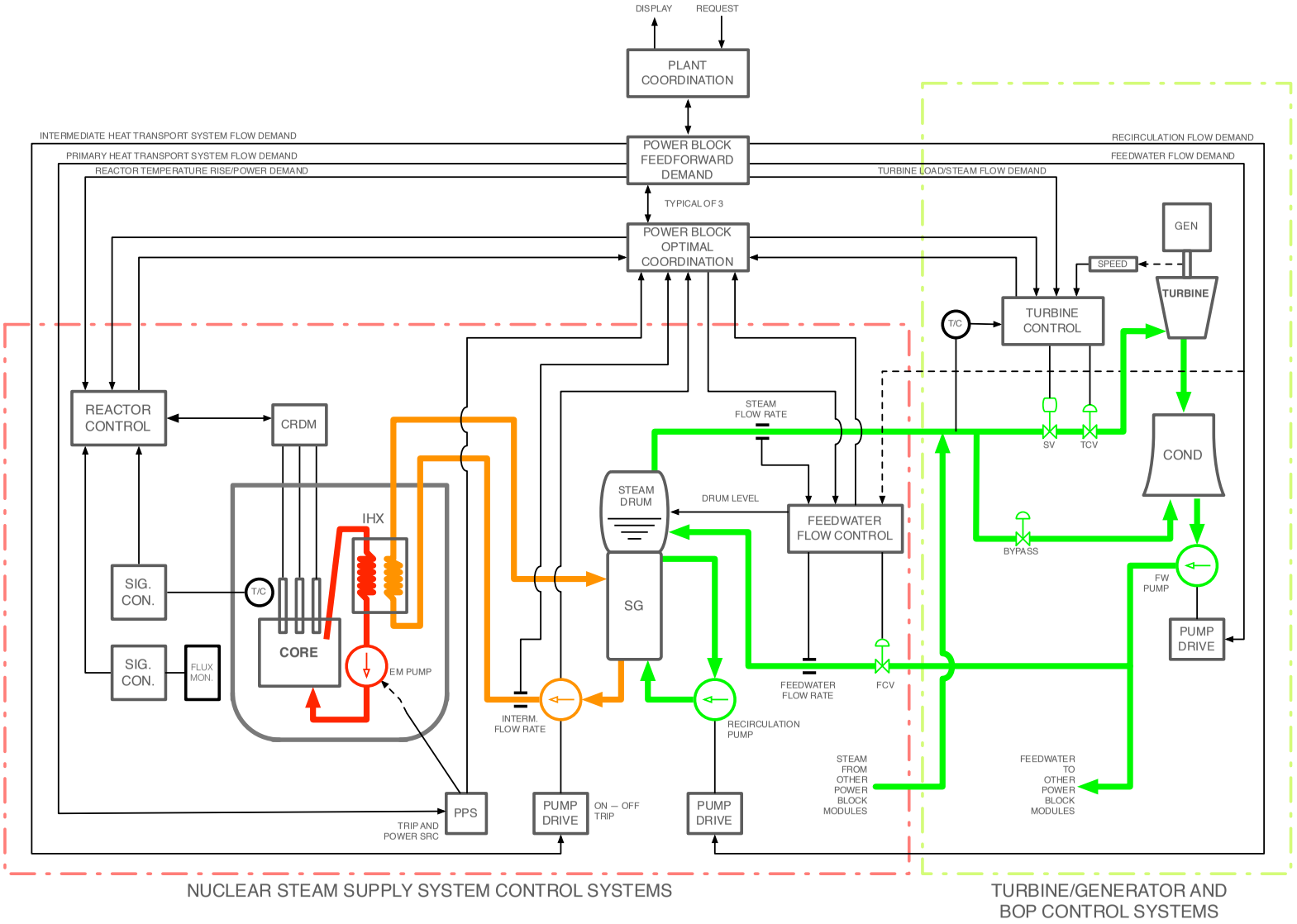


Fig. 31. Illustration of flow of heat from the reactor to the ultimate heat sink (UHS), and Tier-I sensing and actuation interfaces [Redrawn from Fig. 7.11–4 in PRISM Preliminary Safety Information Document, Ref. 9]

It should be noted that this categorization is not based on formal descriptions. Certain components and support systems may straddle more than on tier, particularly for Tier-II and Tier-III systems. As will be seen, classification ultimately is a design decision for the I&C engineer. Architectural decisions have reliability and availability implications; therefore, risk assessments should be adopted as part of the process.

4.7.2 Tier-I Systems and Functions

Tier-I systems are *directly* involved in the heat transport path from the reactor (heat source) to the ultimate heat sink (UHS). The UHS can be a river, lake, sea, or ocean, which is the typical heat sink. It can also be a passive heat dissipation mode that allows heat exchange to the air. Tier-I functions are those performed by Tier-I systems.

A preliminary list of Tier-I systems and associated sensing and actuation interfaces is shown in Table 2.

Table 2. Tier-I systems with sensing and control interfaces for the ALMR PRISM plant

System	Component		Interfaces	
			Sensing	**Control**
Reactor Core	Control Rod Drive Mechanisms[a]		• Servo encoder • Linear variable differential transformer	• Servo motors
	Core Barrel		• In-core source-range flux detectors (3x)	• Reactor startup
	Reactor Vessel		• Short-range level measurement	• Flow rate estimation
Primary Heat Transport System	Electromagnetic Pump (4x)		• Core inlet temperature • Coil current • Coil temperature • Magnetic flow rate measurement	• Drive current to coils (frequency, current, & voltage)
	Upper Plenum		• Core outlet temperature	• Reactor power
	Intermediate Heat Exchanger (2x): Primary side	Inlet	• Core outlet/ IHX primary inlet temperature	• Reactor power
		Outlet	• IHX primary outlet temperature	• Reactor power
Intermediate Heat Transport System	Intermediate Heat Exchanger (2x): Secondary side	Inlet	• Intermediate loop inlet temperature	• Intermediate loop flow rate • Feedwater flow rate
		Outlet	• Intermediate loop outlet temperature	• Intermediate loop flow rate • Feedwater flow control
	Mechanical pump (2x)		• Pump speed measurement	• Intermediate loop flow rate • Pump speed control • Pump on-off control
	Sodium Expansion Tank		• Level measurement	[For indirect calculation of flow rate]
	Steam Generator (3x): Sodium Side		• Temperature measurement	• Reactor power

Table 2. (continued)

SYSTEM	COMPONENT	INTERFACES	
		SENSING	CONTROL
Power Conversion System	Steam Drum (3x)	• Level measurement • Pressure measurement	[Indirect level control by feedwater flow rate]
	Steam Generator (3x): Secondary side	• Steam flow measurement • Steam quality measurement	• Turbine speed • Reactor power
	Recirculation Pump (3x)	• Pump speed	• Steam generator level • Pump speed • Pump on-off
	High-Pressure Feedwater Heater	• Flow	• Reheat flow
	Feedwater Pumps (3x)	• Pump speed • Pump suction • Pump head	• Pump speed
	Feedwater Booster Pumps (3x)	• Pump speed • Pump suction • Pump head	• Pump speed
	Deaerator	• Temperature • Vacuum pressure • Steam flow • Level	• Deaeration steam flow rate • Boiler feedwater flow rate (bypass)
	Low-Pressure Feedwater Heaters (4x)	• Temperature	• Steam flow rate
	Steam Jet Air Ejectors (2x)	• Vacuum/pressure	• Flow rate • Pressure
	Condensate Pumps (3x)	• Temperature • Head and suction pressure	• Pump speed • Bypass valve position
	Condenser	• Level • Temperature	• Vacuum • Ultimate Heat Sink (UHS) flow rate
	Low-Pressure Turbines (2x)	• Steam flow • Temperature	• Steam flow
	High-Pressure Turbine	• Steam flow • Temperature	• Steam flow
	Generator	• Speed • Output current (3φ) • Output voltage (3φ)	• Turbine steam flow • Exciter
	Moisture Separator Reheaters (2)	• Temperature • Pressure	• Reheater steam flow rate

[a]Only grey control rods are considered used for flux regulation. Black rods and diverse shutdown mechanisms are typically safety-grade components that are used for emergency shutdown.

The classification of Tier-I system encompasses safety systems*, safety-related systems, and non-safety-related systems. In many cases, Tier-I systems may have redundant components to perform their assigned functions to reduce the probability of failure. Some of these functions may be performed by diverse systems to minimize common-mode failures.

As noted in Table 2, sensing and control interfaces to Tier-I systems and Tier-I functions are typically related to continuous-time control. Therefore, they are interfaced directly by local feedback loop controls to the integrated control system. Though these interfaces may have significance for the supervisory control system, data from these systems is used to create an accurate snapshot of the state of the plant.

4.7.3 Tier-II Systems and Functions

Tier-II systems *directly* provide support functions for Tier-I systems. Similarly, Tier-II functions are those performed by Tier-II systems. A preliminary list of Tier-II systems and the associated sensing and control interfaces is given in Table 3.

Tier-II systems and functions have particular significance for the supervisory control system: Systems in this tier provide necessary actuation interfaces for event-based control, such as taking a pump off-line while commencing a start-up sequence for a backup pump, or isolating a main flow pipe using an isolation valve and establishing an auxiliary flow path. They also provide additional sensory information for fault diagnostics to establish a holistic status of plant condition based on the health status of critical components.

Table 3. Tier-II systems with sensing and control interfaces for the ALMR PRISM plant

System	Component	Interfaces	
		Sensing	**Control**
Reactor Core	Control Rod Drive Mechanisms[a]	• Drive temperature • Drive power	Cooling set point
	Core Barrel	• Vibration measurement	• Diagnostics
	Reactor Vessel	• Strain gauges • Vibration measurement • Temperature	• Diagnostics
	Guard Vessel	• Continuity detection (for sodium leak)	• Anticipatory trip
Primary Heat Transport System	Electromagnetic Pump (4x)	• Coil temperature	• Anticipatory trip • Diagnostics
	Piping and Interconnects	• Piping temperature • Containment pipe pressure/conductivity	• Trace heating power • Inner piping leak detection
	Cover Gas Cavity	• Gas pressure • Gas temperature • Gas impurity contamination	• Gas flow modulation
	Intermediate Heat Exchanger (2x): Primary side	• Gamma measurement	• Fuel leak detection

* The three-tiered classification system is not a regulatory concept but, rather, is used as an analysis tool to partition plant systems into logical functional zones for the application of supervisory control.

Table 3. (continued)

System	Component	Interfaces	
		Sensing	Control
Intermediate Heat Transport System	Intermediate Heat Exchanger (2x): Secondary side	• Gamma measurement	• Heat exchanger leak detection
	Mechanical pump (2x)	• Coolant temperature and flow • Lubrication flow and pressure • Vibration measurement • Bearing temperature	• Cooling subsystem control (Tier-III) • Lubrication subsystem control • Diagnostics
Intermediate Heat Transport System (cont)	Piping and Interconnects	• Piping temperature • Containment pipe pressure/conductivity	• Trace heating power • Inner piping leak detection
	Sodium Expansion Tank	Level measurement	Make up sodium
	Sodium Dump Tank	• Level measurement	• Overfill protection
	Rupture Disk	• Status (sensing continuity)	• Diagnostics
	Steam Generator (3x): Sodium Side (Shell Side)	• Vibration	• Diagnostics
	Steam Generator (3x): Secondary Side (Tube Side)	• Vibration	• Diagnostics
	Recirculation Pump (3x)	• Pump motor temperature • Bearing temperature • Vibration	• Diagnostics • Subsystem control
	Feedwater Pumps (3x)	• Pump coolant temperature and flow • Lubrication flow and pressure • Vibration measurement • Bearing temperature	• Pump coolant flow control (Tier-III) • Diagnostics
	Feedwater Booster Pumps (3x)	• Pump coolant temperature and flow • Lubrication flow and pressure • Vibration measurement • Bearing temperature	• Pump coolant flow control (Tier-III) • Diagnostics
	Condensate Pumps (3x)	• Coolant temperature and flow • Lubrication flow and pressure • Vibration measurement • Bearing temperature	• Pump coolant flow control (Tier-III) • Diagnostics
	Low-Pressure Turbines (2x)	• Bearing temperature	• Bearing lubrication and cooling control •
	High-Pressure Turbine	• Bearing temperature	• Bearing lubrication and cooling control

Table 3. (continued)

System	Component	Interfaces	
		Sensing	**Control**
Intermediate Heat Transport System (cont)	Generator	• H_2 pressure • Bearing temperature • Exciter current • Exciter voltage	• H_2 makeup • Exciter control
	Demineralizer	• Pressure drop	• Valving alignment
	FW turbine lubrication, gland, and seals	• Pressure • Temperature • Leakage rate	• Lubrication and cooling • Diagnostics
	Condensate pump gland & seals	• Leakage rate	• Diagnostics
	Chemical addition system	• pH • Conductivity	Chemical mix addition

[a]Only grey control rods are considered used for flux regulation. Black rods and diverse shutdown mechanisms are typically safety-grade components that are used for emergency shutdown.

4.7.4 Tier-III Systems and Functions

Tier-III systems provide common services that supply bulk materials, energy, or data to the Tier-I and Tier-II systems. Tier-III functions are those performed by Tier-III systems.

A partial list of the Tier-III systems is as follows:

1. plant electrical,
2. fire protection,
3. sodium fire protection,
4. service water (of which there are several classes),
5. gas supply—e.g., argon, helium, nitrogen, compressed air and instrument air,
6. building environment—e.g., heating, ventilation and air conditioning (HVAC),
7. hydraulic supply,
8. auxiliary steam supply,
9. radioactive waste handling, and
10. fuel handling.

As indicated earlier, the distinction between Tier-II and Tier-III systems may be obscure for certain systems. The key distinction of a Tier-III system lies in the fact that it does not offer any control options for the operator in the event of loss of availability or reduced performance.

Instrument air supply system can be used as an example. Instrument air is used across the plant for the operation of various components, such air-operated valves. Some of these components can even be safety related. However, this system typically does not provide control interfaces in the main control room. In the event of a failure, the system indicates its failed status, which will cause an alarm in the control room. However, operators do not have many options when the instrument air system fails other than shutting down the reactor, because it supplies critical material for Tier-II systems. It should be noted that a failure in a Tier-III level can cause subsequent failure or upset in a Tier-I or Tier-II system.

As an example of Tier III failure propagation, in the AP600 probabilistic risk assessment (PRA), loss of component cooling water, service water, and compressed air initiating system events are defined as *special initiating events*. Special initiating events typically result in a reactor trip and affect the

performance of the front-line systems—that is, normal residual heat removal, passive residual heat removal, core makeup tank, and main and start-up feedwater. Identification of these initiators is performed by reviewing the plant design, support system, and abnormal operating procedures.

As yet another example, in the PRA for the Economic Simplified Boiling Water Reactor (ESBWR), *special initiating events* refer to plant-specific systemic malfunctions that can lead to a plant trip. A new initiating category is identified when the event is not associated with any of the categories defined before; otherwise, it is grouped into one of the defined categories and the frequency of the existing category is modified to account for the contribution of the systemic malfunction. In general, all systems that can influence the parameters involved with the scram or isolation signals—either directly or as a consequence—are analyzed. The list of systems analyzed is as follows:

Front-line systems:

- Control rod drive (CRD) system
- Feedwater, condensate
- Isolation Condenser System (ICS)
- Depressurization system (DPV/SRV)
- Gravity-Driven Cooling System (GDCS)
- Fuel and Auxiliary Pool Cooling (FAPC) system
- Reactor Water Cleanup (RWCU) and Shutdown Cooling System (SDCS)
- Standby Liquid Control System (SLCS)

Support Systems

- Reactor Component Cooling Water (RCCW) system
- Turbine Component Cooling Water (TCCW)
- Plant Service Water System (PSWS)
- Air systems (HPNSS, Service Air, Instrument Air)
- 13.8 kVAC and 6.9 kVAC bus system
- 250 kVDC bus system
- Reactor Water Level Instrumentation (RWLI) system
- Drywell Cooling System (DCS)

Figure 32 shows how the PRSIM plant systems are broken down into the tiered structure, as discussed previously. It should be noted that the systems indicated in the Fig. 32 are generalized over those of the previous tables. For each of these systems, the possibility for the generation of scram or isolation signals due to spurious actuation or a variation of the system configuration resulting from a human error or hardware failure is investigated. The effect of pipe break in these systems is also considered.

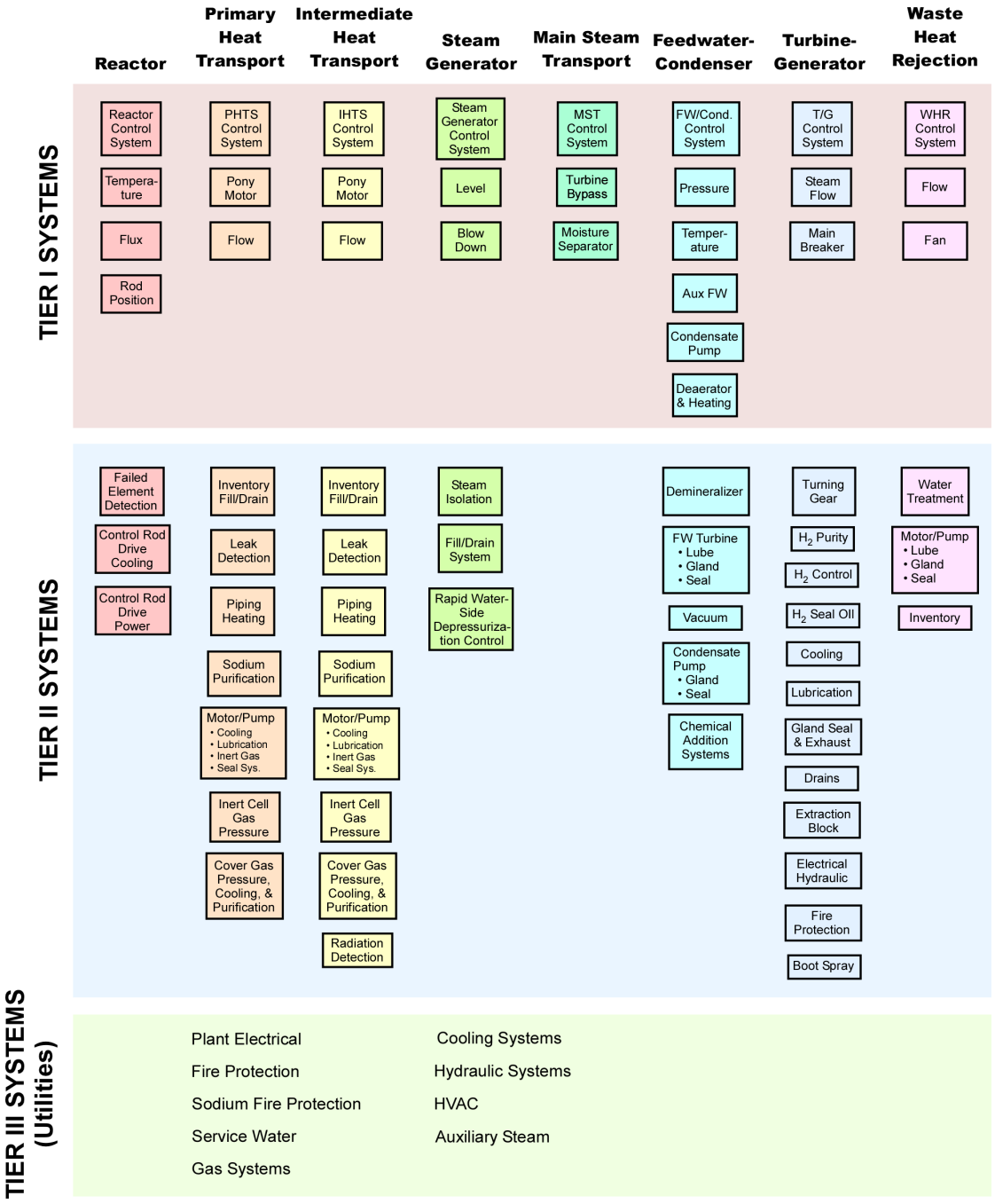


Fig. 32. Summary breakdown of major plant systems in tiered structure as defined.

A generic reactor primary coolant pump is shown in Fig. 33 illustrating its relationship to the tiered functional taxonomy. The only component of the pump that is Tier-I controlled is the main motor drive (stator windings and rotor shown in red). The motor control shown is binary—off or on; likewise, a variable speed drive would also be part of Tier-I motor control. Examples of the pump's Tier-II systems (shown in blue) are oil lift pump, numerous temperature, pressure, flow rate, level, and vibration measurements. Note that there is an oil lift pressure sensor (Tier-II) that interlocks with Tier-I motor circuit breakers. The coolant pump also interfaces with Tier-III systems for component cooling water (shown in green).

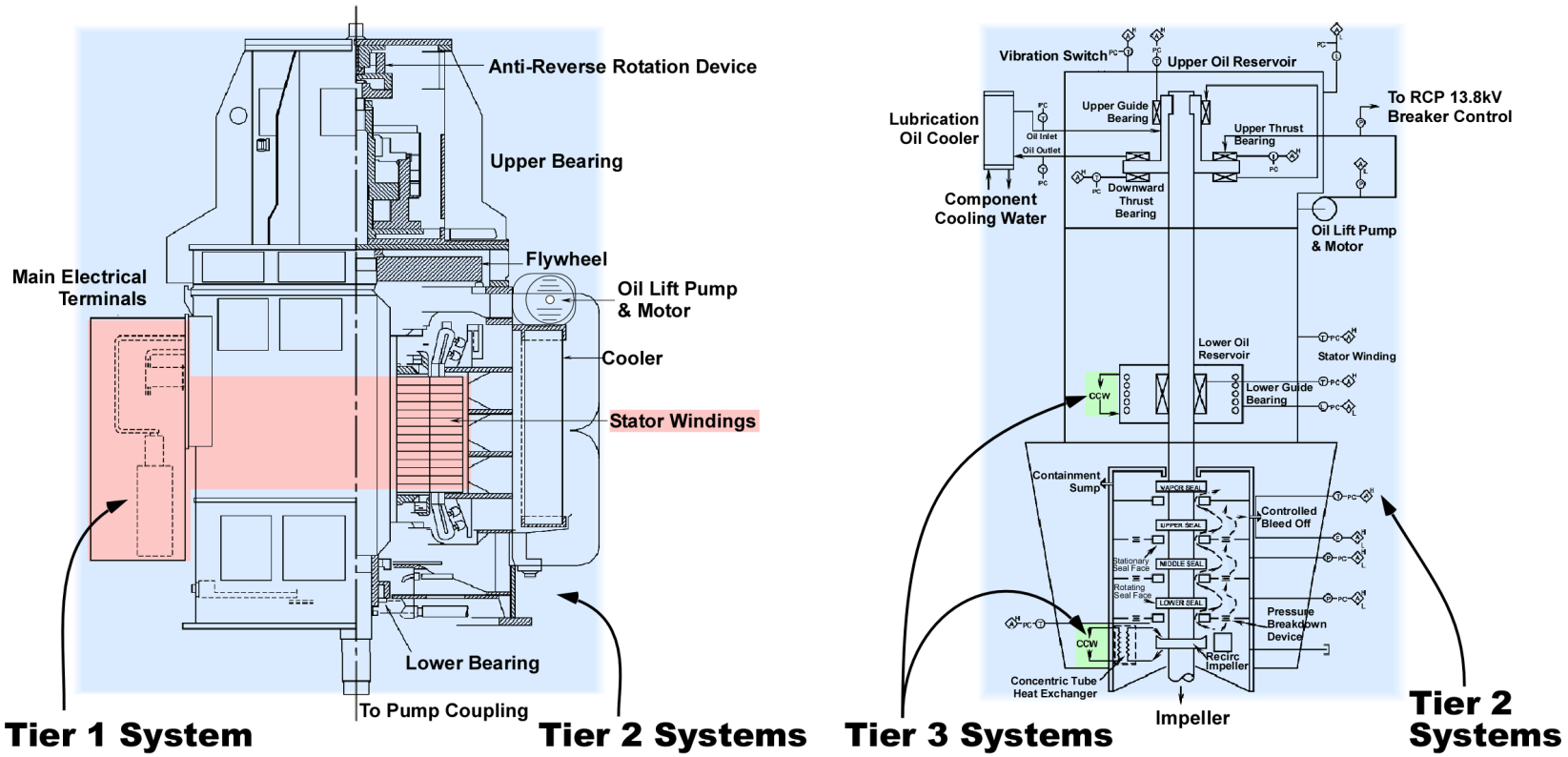


Fig. 33. Illustration of a component having membership in all three tiers.

The modular-designed, multi-unit plants have more and stronger dependencies among systems than primarily single-unit plants at a common site. In fact, the design philosophy of the modular multi-unit plants is to form a single power plant station with respect to power generation and control. This philosophy is readily apparent with the single turbine-generator shared among three reactor modules for the ALMR PRISM power block, as shown in Fig. 14.

4.8 ALLOCATION OF FUNCTIONS

Highly automated control involves more than simple automation of routine functions. It implies the detection of conditions and events, determination of appropriate responses based on situational awareness, adaptation to unanticipated events or degraded/failed components, and reevaluation of operational goals.

As illustrated in Fig. 34, functions necessary for reliable operation of the plant are allocated between the human operator and automation agents. Allocation of functions requires careful evaluation of work conditions and task loads and requires precise balance between reducing operator workload and maintaining his or her involvement in operations. The functional allocation of tasks between the human operator and automation defines the boundaries of the supervisory control system, and drives its requirements specification process.

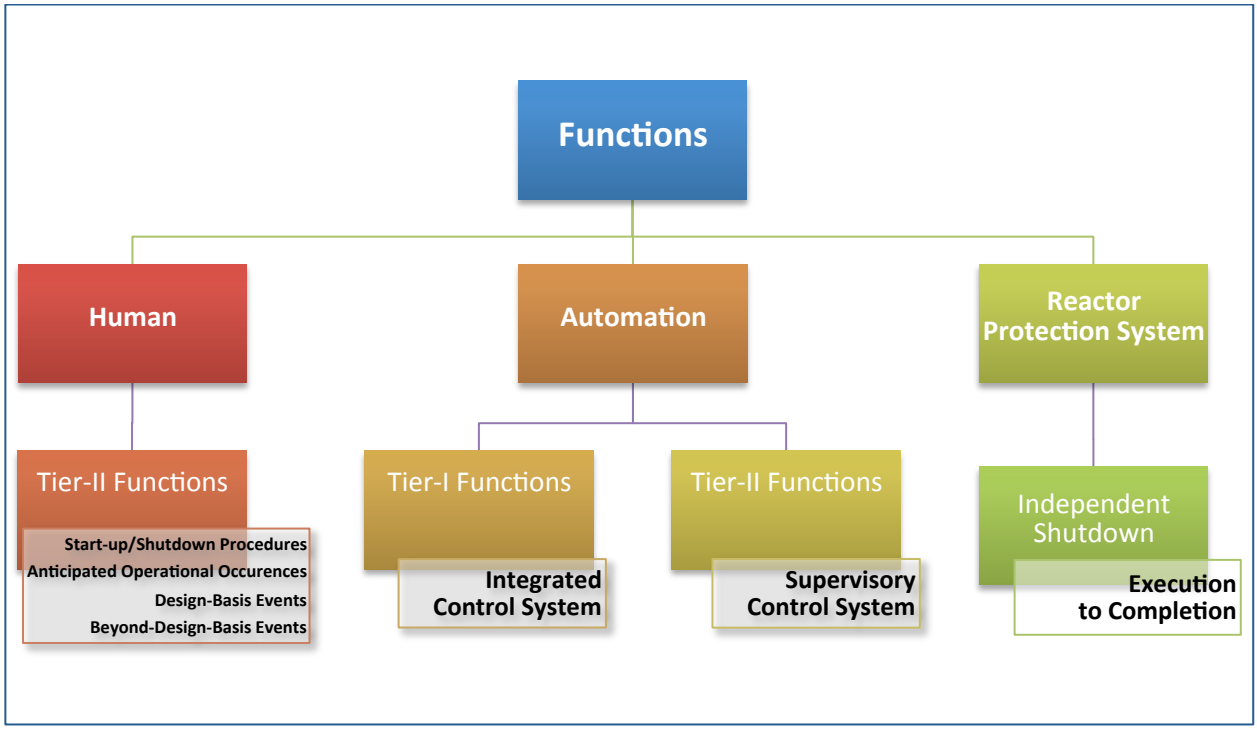


Fig. 34. Allocation of functions between humans and automation in concepts of operations.

Supervisory control provides a means for the integration of control, diagnostics, and decision to support extensive automation. The architectural framework and foundational modules that are needed to facilitate the integration of control, diagnostics, and decision to support the necessary level of automation extend the capabilities of an integrated control system (ICS) at a reactor module (RM) level, and provide new capabilities at the power block (PB) and plant levels.

The overall plant control strategy includes three distinct control systems:

1. Integrated control system (ICS),
2. Supervisory control system (SCS), and
3. Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS).

Figure 35 shows the master logic diagram (MLD) for integrated and supervisory control at the RM level. The top level of the MLD shows that there are only two categories of operation: normal and off-normal conditions. When operating normally, the ICS is in control of the PB/RM, with the SCS performing diagnostics and, if necessary, modifying operating conditions or equipment. Off-normal conditions may be created by an upset in a Tier-I or Tier-II system, which can be corrected by the ICS or SCS, or it may be an upset that necessitates a safety system intervention.

Defining the role of supervisory control is a matter of determining the desired degree of automation and reassigning functions and decision-making roles from human operators (licensed operators, roving operators, and maintenance personnel) to computer-driven systems. The reassignment is not as simple as mechanizing operating procedures as discussed previously since human operators supply diagnostic, prognostic, and high-level decision-making capabilities. Figure 36 shows a mapping of hierarchical decision-making and control architecture layers to the three plant system tiers. The figure illustrates the reassignment of human supervision and decision-making.

Local real-time controllers (PID or other feedback controllers) are employed at the functional level for Tier II and Tier III systems and equipment. The fleet of these local control devices in a plant is numerous. For Tier I systems, the coordination and functional control actions are handled by the integrated control system, which copes with normal and some off-normal events. The Integrated control system has far fewer input and output points than the local control loops.

The supervisory control system has monitoring and control activities present in all tiers because it is controlling heat (power) balance for the multiple reactors and power blocks, coordinating numerous support system states, and coordinating maintenance activities. The supervisory control system in this illustration has displaced many of the operator functions. Without the supervisory control system, much of the diagnostics and decision-making would be in the domain of human operators.

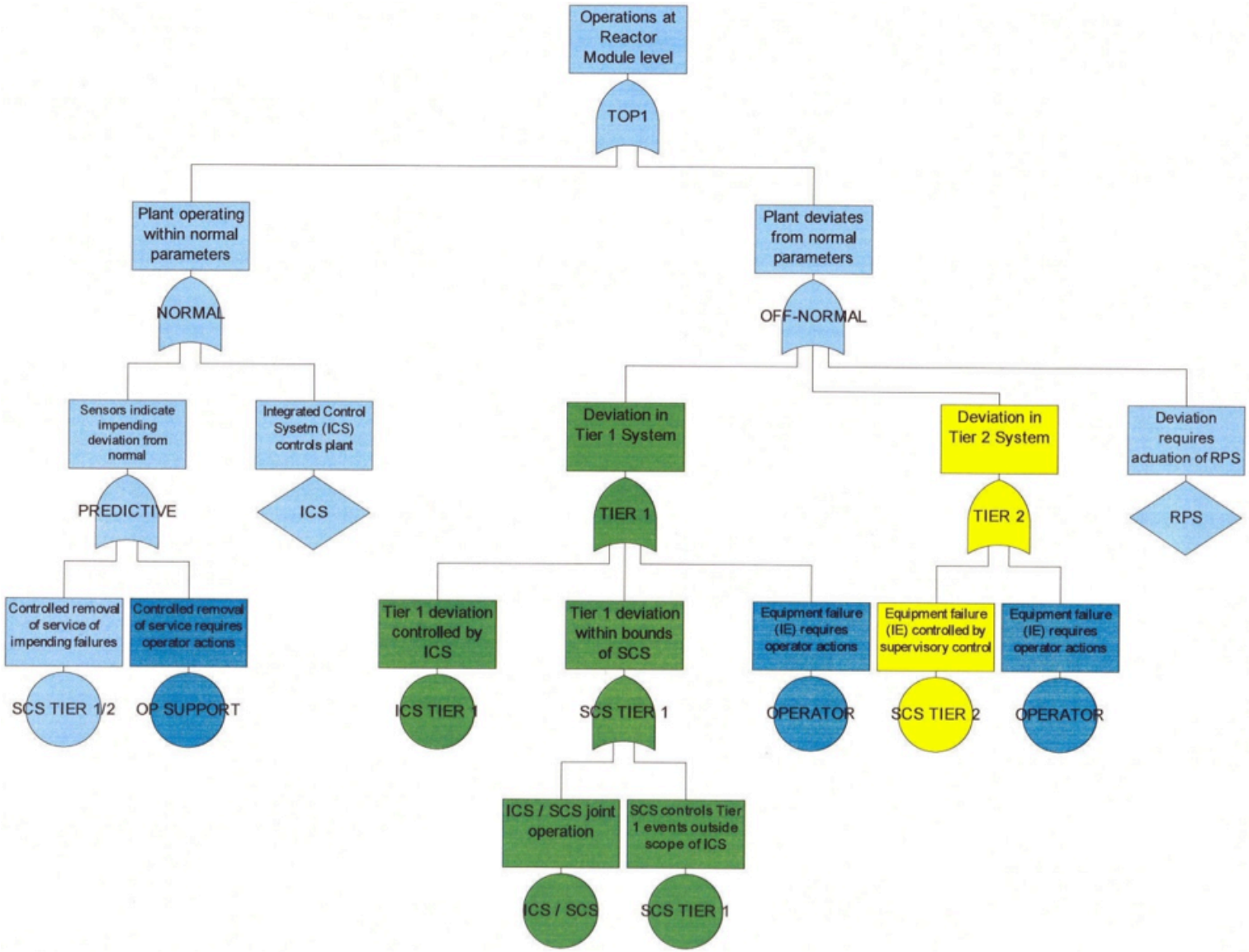


Fig. 35. Master logic diagram for the continuous-time control and supervisory control systems at the reactor module level.

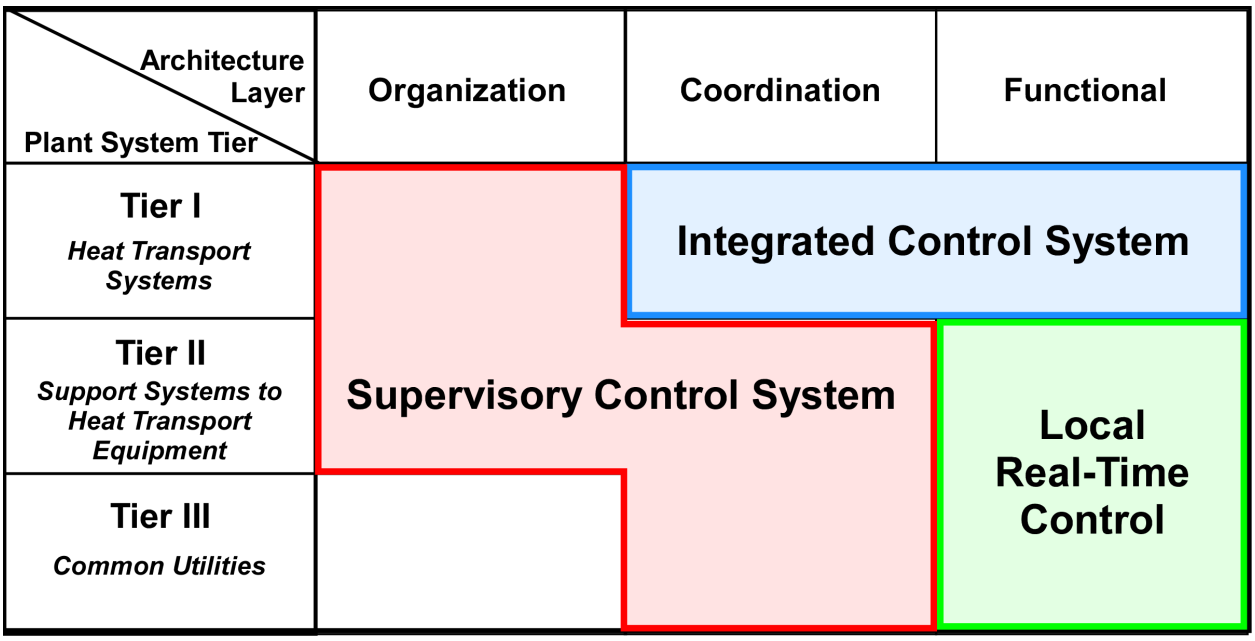


Fig. 36. Mapping of architectural layers of control to plant system tiers.

4.8.1 Integrated Control System

The name *integrated control system* (ICS) is used to convey the capabilities of current-generation control systems, projected onto AdvSMRs.

The ICS maintains plant parameters by matching megawatt generation with plant conditions. This is accomplished by balancing heat loads throughout the Tier-I systems. Thus, the ICS ensures that heat generation and heat removal are matched with appropriate parameter values.

The ICS for a RM provides simultaneous control of

- turbine load, MW(e),
- turbine bypass valves and atmospheric dump valves,
- feedwater control valves,
- main feedwater pump speed, and
- control rod position.

The ICS also allows the reactor module to automatically maneuver from 15–100%, with up to 5% per minute.

For an example, the ICS for a Babcock & Wilcox (B&W) nuclear power plant accomplishes balancing MW(e) generation and plant conditions via four subassemblies[·]:

- *Unit Load Demand* (ULD) functions as a megawatt electric setpoint generator for the ICS.

[·] U.S. Nuclear Regulatory Commission, Human Resources Training & Development, Pressurized Water Reactor B&W Technology Cross-training Course R-326C, Chapter 19.0, Rev. 4, "Transients and Instrument Failures," 2011.

- *Integrated Master* (IM) receives the megawatt setpoint from the unit load demand to control the electrical output of the turbine generator. In addition, the integrated master translates the megawatt demand into signals for feedwater and reactor control.

- *Feedwater Demand* action converts the megawatt demand signal to a feedwater demand in the IM and controls the amount of feedwater supplied to the once-through steam generators.

Reactor Demand action moves the reactor's control rods in or out in response to the megawatt demand signal, and also controls the average reactor coolant system temperature.

The ICS is designed to respond to transients and instrument failures. For example, the B&W nuclear power plants automatically respond to the following transients[·]:

1. loss of one reactor coolant pump,
2. load rejection,
3. reactor trip,
4. power range ex-core neutron instrumentation failure,
5. reactor coolant system loop temperature instrument failures,
6. reactor coolant system loop flow instrument failure,
7. feedwater loop flow instrument failures,
8. loss of one main feedwater pump, and
9. dropped control rod assembly.

However, because some of these transients currently require operator intervention, the addition of the SCS would take over these responsibilities.

4.8.2 Reactor Protection System

There are some off-normal events, such as a seismic event, that initiate the RPS. No integrated or supervisory control is or would be available for these types of events.

4.8.3 Supervisory Control System

The supervisory control system operates at the overall plant level, power-block (PB) level, and reactor-module (RM) level. The PB- and RM-level supervisory control systems are responsible for balancing electrical output and thermal heat loads by providing proper setpoints to associated subsystems of the ICS, while the plant-level supervisory control system—also called the master supervisory control system—is responsible for long-term planning, scheduling, and responding to dispatch requests.

4.8.3.1 Master Supervisory Control System (M-SCS)

The ALMR PRISM control system uses model-based optimal controllers for improved plant operation. These controllers are more robust and provide improved capability of responding to and terminating upset events. Conventional proportional-integral controller models have been used previously in ALMR PRISM simulations studies and have demonstrated the feasibility of multi-module control for various events and power levels. The new optimal controllers now being developed have shown improved

[·] U.S. Nuclear Regulatory Commission, Human Resources Training & Development, Pressurized Water Reactor B&W Technology Cross-training Course R-326C, Chapter 19.0, Rev. 4, "Transients and Instrument Failures," 2011.

performance under simulated testing. These controllers are directed by improved block- and plant-level supervisory controllers, which utilize fault diagnostics and knowledge of the current and desired final operating conditions to select the proper plant operating strategy*.

4.8.3.2 Power-Block-Level Supervisory Control (SCS-PB)

During normal base-load operation, all modules in a block will likely be operated as a unit, and all module power changes will be equal. However, during refueling or during transients, which limit power from a single module, power levels from unaffected modules are varied independently through supervisory control strategies to improve plant availability.

However, similar to the ICS, the SCS will allow the RCS to be operated with unequal loop flows within and between reactor modules.

Operating a nuclear power plant at a constant power level is simpler and less demanding on the plant's equipment and fuel. However, the capability to operate with unequal loop flows will allow plants to "load-follow" and to respond to load change transients. This is important because the growing deployment of intermittent sources of electric power generators has introduced significant and irregular variations in the power supply and has made balancing electricity supply and demand increasingly difficult. For example, because of the sudden influx of large amounts of wind power, some German utilities have started operating their nuclear power plants in load-following mode [10].

The design of the RCS for the AP1000 enables daily load-follow operation with a minimum of manual control by the operator [11]. Automatic reactor power and power distribution control are the basic functions of the RCS. These capabilities are accomplished without a reactor trip or steam dump actuation. Separate control rod banks are used to regulate reactor power and power distribution.

Tennessee Valley Authority (TVA) has indicated that load following is a factor in meeting grid power demands in the Tennessee Valley.

4.8.3.3 Reactor-Module-Level Supervisory Control (SCS-RM)

The ICS maintains the plant within the transition corridor by balancing the electrical and heat load requirements using the Tier-I systems. The ICS does not provide predictive corrections in Tier-I or Tier-II systems and does not provide reactive corrections to failures in Tier-II systems.

Predictive Mode of Operation

Digital systems—and not only safety systems—should include self-diagnostic capabilities to aid in troubleshooting. Fault detection and self-diagnostics are means that can be used to assist in detecting partial system failures that could degrade the capabilities of the computer system, but may not be immediately detectable by the system.

Currently, hardware or software failures detected by self-diagnostics place a protective function into a safe state or leave the protective function in an existing safe state. Similarly, diagnostics at the SCS-RM level will monitor hardware and software, identify imminent failures via monitoring (e.g., excessive

* PRISM PSID GEFR-00793 Dec. 1987, Appendix G Amendment 12 (March 1990).

vibration, temperature), and realign equipment, reduce power, and/or take the soon-to-fail equipment out of service in a controlled manner rather than a response to the failure.

Reactive Mode of Operation

Control systems in operating nuclear power plants currently respond to failures in Tier-I systems. The ICS does not control equipment in Tier-II systems, although the failure or fault in a Tier-II system can translate into the loss of a Tier-I system. The SCS-RM will be capable of event-based functions, such as starting/stopping pumps, opening/closing valves, etc., in Tier-II systems to maintain the heat balance requirements in the Tier-I systems.

4.9 SUMMARY—CHAPTER 4

The key objective of the supervisory control system is to reduce cognitive load on reactor operators by conducting routine operator actions executed primarily during normal operations, and some actions performed during startup and shutdown. The supervisory control system acts in concert with lower levels of control to create an automated system. The targeted level of autonomy for supervisory control of an AdvSMR lies between 5 and 9 on the scale proposed by Sheridan.

To automate a large-scale system, the control of both discontinuous (off-on or state oriented) and continuous (feedback controlled such as PID) systems must be integrated to carry out the functions required to achieve the goals and objectives of the entire plant. The control architecture proposed is an hierarchical configuration consisting of a functional layer, coordination layer, and an organization layer arranged to suit the three-tier division of the plant: Tier 1 systems are directly involved in the heat transport path from the reactor (heat source) to the ultimate heat sink. Tier 2 systems directly provide support functions for Tier-I systems (but are not themselves in the mainstream flow of energy from reactor to generator). Tier 3 systems provide common services that supply bulk materials, energy, or data to the Tier-1 and Tier-2 systems.

The internal mechanisms of supervisory control comprise decision-making functions that work to steer the functions and configuration of lower level controllers. A master logic diagram is developed that shows the relationship between supervisory control and the ICS, which maintains plant parameters by matching megawatt generation with plant conditions. Under normal operations, and in the 15–100 percent power range, the ICS controls turbine load, turbine bypass valves and atmospheric dump valves, feedwater control valves, main feedwater pump speed, and control rod position. The supervisory control system operates at the overall plant level, power-block (PB) level, and reactor-module (RM) level. A principal function of the supervisory control is to set high level goals for the ICS and other lower level controllers and in particular to diagnose current malfunctions and predict future problems to keep the plant in operation, away from protection systems action, and coordinate maintenance activities.

4.10 REFERENCES – CHAPTER 4

1. T. B. Sheridan, *Telerobotics, automation, and human supervisory control*, The MIT Press, Cambridge, Massachusetts (1992).
2. R. A. Kisner and G. V. S. Raju, *Automating Large-Scale Power Plant Systems: A Perspective and Philosophy*, ORNL/TM-9500, Oak Ridge National Laboratory (December 1984).
3. A. M. Meystel and J. S. Albus, *Intelligent Systems: Architecture, Design and Control*, Wiley Series on Intelligent Systems (2002).
4. S. V. Amari, H. Pham, and G. Dill, "Optimal Design of k-out-of-n:G Subsystems Subjected to Imperfect Fault-Coverage," *IEEE Transactions on Reliability*, 53(4) (December 2004).
5. W. Torres-Pomales, *Software Fault Tolerance: A Tutorial*, NASA/TM-2000-210616 (Oct. 2000).

6. M. D. Muhlheim et al., "Evaluation of I&C Architecture Alternatives Required for the Jupiter Icy Moons Orbiter (JIMO) Reactor, Transactions of the American Nuclear Society, ANS Winter Meeting, Albuquerque, NM (November 2006).
7. J. B. Cobble et al., *Technical Needs for Enhancing Risk Monitors with Equipment Condition Assessment for Advanced Small Modular Reactors*, PNNL-22377, Rev. 0, SMR/ICHMI/PNNL/TR-2013/02 (Apr. 2013).
8. HTGR Technology Course for the Nuclear Regulatory Commission, *Module 12, "Instrumentation and Controls (I&C) and Control Room Design,"* Idaho National Laboratory and General Atomics, May 24-27 (2010).
9. *PRISM Preliminary Safety Information Document*, GEFR-00793, UC-87Ta, Prepared for US Department of Energy under Contract No. DE-AC03-85NE37937 (December 1987).
10. A. Lokhov, NEA News, "Load-following with nuclear power plants," OECD NEA, *NEA-News*, Vol. 29, No. 2 (2011).
11. Westinghouse Electric Company LLC, *AP1000 Design Control Document*, Ch. 7, "Instrumentation and Controls," Rev. 15, 2005.

5. ANALYTICAL LIMITS FOR SUPERVISORY CONTROL

The supervisory control system strives to maintain plant parameters from reaching trip setpoints. Typical RPS setpoints and measurements are provided in Table 4. A goal of control design is to build in both of the properties of fault tolerance and resilience.

Table 4. ALMR PRISM RPS setpoints, measurements, and instrumentation

RPS setpoint parameters	Physical measurements	Instrumentation
Reactor power	Neutron flux	• Flux monitor in drywells in concrete silo
Sodium flow rate	• EM pump discharge pressure • Differential sodium level	• Strain gauge instrumented diaphragm pressure transducers in discharge manifold of each of the four EM pumps • Level sensors
Reactor power-to-flow ratio	Neutron flux/sodium flow rate	• Same as above
Reactor inlet sodium temperature	Sodium temperature	• four thermowells—each containing four sensing elements—attached to the upper internal structure
Reactor outlet sodium temperature	Sodium temperature	• 1 drywell—containing 4 sensing elements at the outlet of each of the four EM pumps
Reactor sodium level	• Long-range level • Short-range level	• Heated thermocouple • Microwave radar • Ultrasonic guided wave • Differential pressure • Capacitance
Turbine status	Trip signal	• Loss of sync with grid • Loss of hydrogen cooling • Turbine overspeed • Vacuum status

One means of achieving system-wide fault tolerance and resilience is to provide good control for the plant operating in normal or nearly normal conditions and also to provide monitors that accommodate various stages of degradation of equipment or equipment interfaces. The regions of operation are defined in Table 5.

The method is based on a hierarchically structured control system. At the top of the pyramid are the RPS setpoints. Feeding into the RPS setpoints are those conditions or variables that can be controlled to drive the system out of the degraded region back into the homeostatic region. These in turn lead to systems and components that can be controlled via local controllers. For example, a high outlet temperature from the reactor core can be lowered by decreasing power, reducing the coolant inlet temperature, and increasing secondary side flow rate. Each of these can be adjusted using plant controls. Inserting the control rods, increasing coolant flow, etc., are means to reduce core thermal power.

Table 5. Typical operating regimes for nuclear reactors. (See Figs. 37 and 38 for illustration of the homeostatic, degraded and uncontrollable regions.)

Known conditions of the plant	Description
Normal operations	Operation anywhere within the homeostatic region is considered normal. Strategies for optimal control and adaptive control are employed when the system is situated in the homeostatic control region.
Limiting conditions of operation (LCO)	The control objectives of the degraded region are to (1) maintain continuous and uninterrupted delivery of principal products of the system if possible; (2) prevent or minimize equipment damage; and (3) avert intervention by the plant safety and protection systems by maneuvering the system away from the envelope inscribed by the safety systems.
Abnormal operations	A goal of the control system upon entering the uncontrollable region is to alert the plant operators that a problem in controllability exists. Prior to entering this region, the control system should have been attempting to shut down or subdue the process. Entry into this region is an indication that the procedures or rules used while in the degraded region *were* ineffective. Further, the control system may have exhausted its ability or resources to control or restrain the situation. Surrounding the uncontrollable region are the initiators for the plant safety and protection systems. Failure of the control system to regain control of the process should eventually invoke a safety-system actuation. However, the failures or damage that impeded control action, hence led the system to the uncontrollable region, also could possibly prevent effective safety action.

5.1 NORMAL OPERATING CONDITIONS

Reactor power systems are considered in normal operation when all Tier-I systems are operating within their rated performance region and energy flow is balanced between reactor and heat sinks (i.e., generated electrical power and ultimate heat sink). In normal operation, the upper levels of hierarchical supervisory control are not communicating new commands to the integrated control system (ICS); the ICS is maintaining operation about the target, as illustrated in Fig. 37. Any wandering about the target is contained within the homeostatic region.

Normal operation is also possible during transitions such as ascending to a new power level, as illustrated in Fig. 38. The ICS is able to maintain trajectories as commanded by the supervisory control system as long as all participating components, subsystems, and their associated controllers are functioning within their respective rated performance region. During steady state and transition, no intervention by the reactor protection systems is necessary. However, as indicated in Fig. 38 an event of sufficient consequence can drive the operating state (whether in transition or at steady state) out of the control region of the ICS and into a degraded region or, further, to the point of reactor protection system intervention. It is in the regions that surround the homeostatic region of the ICS that the supervisory control system issues commands necessary to prevent further excursion toward reactor trip or equipment damage.

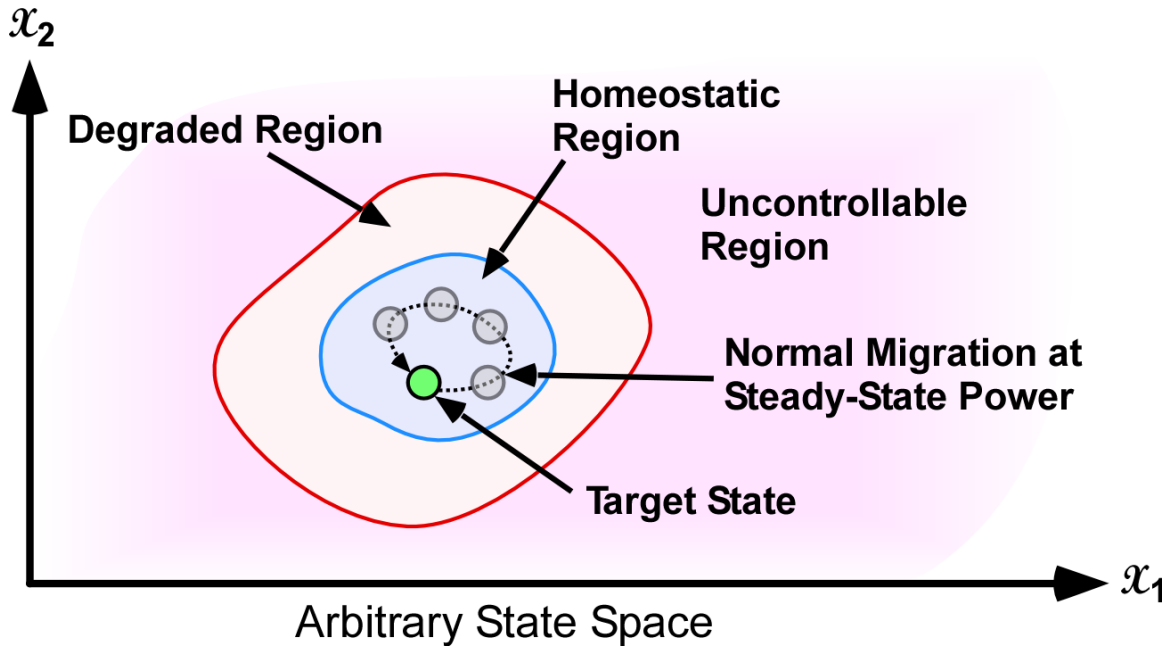


Fig. 37. Illustration of steady-state operation in the normal region of arbitrary parameters x_1 and x_2 for a large-scale complex system.

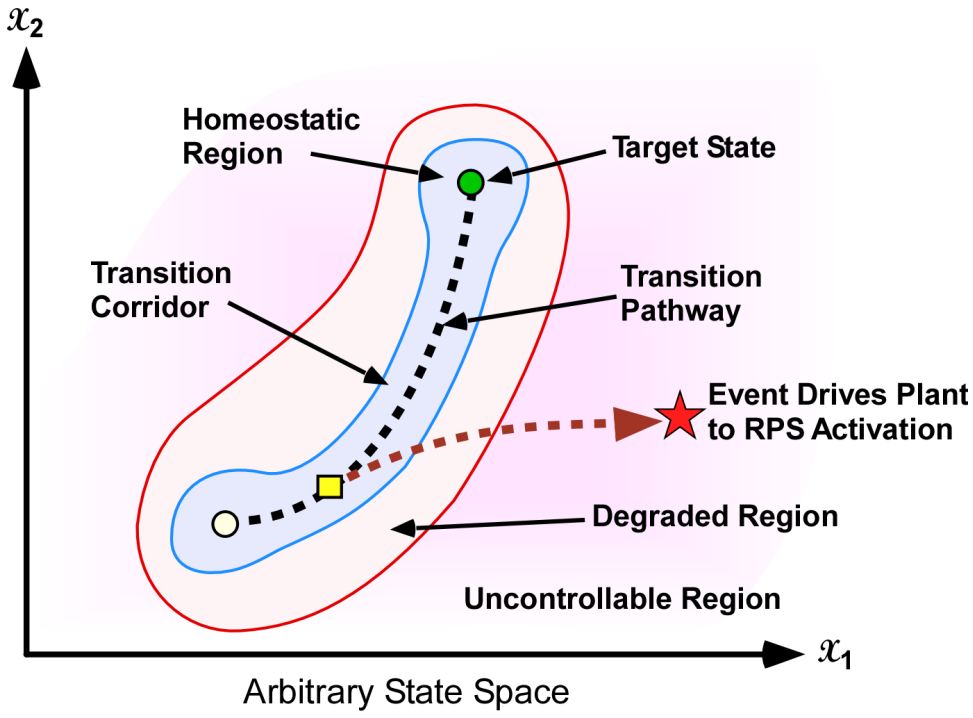


Fig. 38. Illustration of a possible state transition in arbitrary parameters x_1 and x_2 in a large-scale complex system.

The goal of control within the homeostatic region is to effect production of the desired outputs of the controlled plant system. In the absence of major equipment failure, behavior in this region tends to converge on the target state, which is the desired operating state. Strategies for optimal, adaptive, and other control types are employed in the homeostatic control region. As appropriate for the mode of control, various criteria may be chosen to meet minimum error, time, energy, or mechanical stress in

controlling the system. Power plants often change states because of maintenance schedules, load demand changes, and refueling schedules.

To accomplish transition from current state to desired state, a preferred pathway is established and a corridor that surrounds the pathway for the transition is established. The determination of the target pathway and the rates of change along the pathway is based on optimization calculations because alternative pathways may offer differing energy efficiency, power demands, mechanical or thermal component stress, time to completion, or margin to safety actions. Real-time identification of the best transitions is part of the supervisory control system's capability. Operation within the homeostatic region is considered normal. Some minor faults in equipment or their interconnections are tolerated within the homeostatic region as long as the capability of the control system to maintain the target state has not been compromised.

5.2 ABNORMAL OPERATIONS

The goal of supervisory control when the plant enters the degraded region is to prevent further migration into the degraded region and take steps to instigate restoration of failed systems so that return to the desired target state may proceed. Should the original target state be unattainable, the supervisory control identifies a new target state appropriate to the current plant condition and sends commands to drive the ICS along the newly prescribed path. This can be summarized as follows:

- Maintain continuous and uninterrupted (perhaps reduced) delivery of power
- Prevent or minimize equipment damage
- Avert intervention by the plant safety and protection systems

Three types of crises are possible with in the degraded region (adapted from [1]):

1. *Stability Crisis*. This crisis describes a controlled system that has become unstable. The strategy is to maneuver the system to an intermediate safe and stable state that is near the original target state while continuing to produce power. The strategy allows Tier-I systems to remain on-line although at a reduced level if necessary.

   An example of stability crisis at component level would be a valve controller malfunction that has introduced flow and pressure oscillations in a component-cooling stream that threatens to affect Tier-I systems. By reducing heat generated, for which the component cooling is required, further propagation of the problem can be halted. A temporary solution may be to bypass the malfunctioning control valve through an alternate flow channel (perhaps at reduced flow rate).

2. *Viability Crisis*. The crisis describes the case in which no stable state can be found. Hence, it would be necessary to reduce power output to zero until a solution is implemented.

   Continuing the previous example, the flow path for component cooling water has no alternative. The induced temperature fluctuations resulting from the malfunctioning controller-valve combination is causing substantial deviation from setpoint to the Tier-I system. The only alternative is to shut the process down for repair.

3. *Integrity Crisis*. This crisis describes a system approaching imminent equipment damage or reactor protection trip threshold. The strategy is to invoke immediate action to protect equipment and subsystems.

From the previous example, the component coolant flow control valve has frozen shut, stopping all coolant to a Tier-I component. No other means of cooling is available. Therefore, without delay, an immediate reduction in power would be commanded.

The normal plant response to an anticipated transient requiring scram depends upon the nature of the transient. For example, in a high-temperature gas-cooled reactor (HTGR), in most cases, the normal plant response involves reactor trip in one or more modules, followed by decay heat removal through the heat transport system of the tripped modules [2]. If, for example, one power conversion system (PCS) train fails when all four modules are at full power, the normal plant response is to trip two modules and use their heat transport systems to convey decay heat from their reactor cores to the operational power conversion system train.

The supervisory control system through its prognostic capability and scheduling strategies can identify alternative target states when crisis events as described above occur. The *look-ahead planning* is illustrated graphically in Fig. 39. Here is shown a system at one state progressing to a target state along a prescribed path as previously discussed. An event occurs that prevents further safe and cost-effective progress along the original pathway. The supervisory control system established a new target based on knowledge of the plant and the nature of the original target and defines a new pathway. All along the pathway estimates are made as to possible deviations, as shown by the projection triangles. The process is similar to storm path prediction by forecasters during inclement weather.

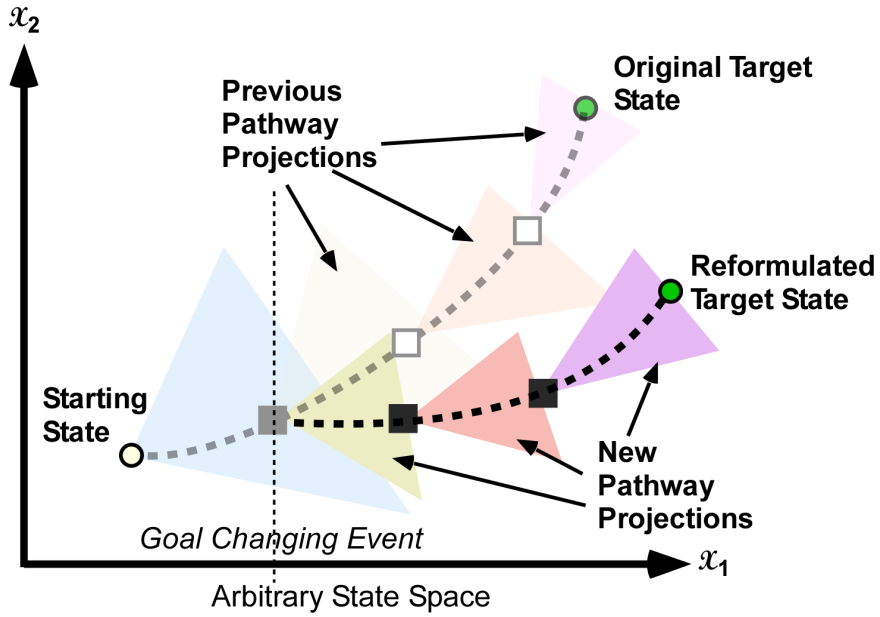


Fig. 39. Illustration of predictive-corrective nature of decision-making.

5.3 LIMITING CONDITION FOR OPERATION

Limiting condition for operation (LCO) is a formal definition from Technical Specifications that identifies the lowest functional capability or performance level of equipment required for safe operation of the facility.

Trip setpoints are chosen to ensure that a trip or safety actuation occurs before the process reaches the Analytical Limit (AL). Trip setpoints are also chosen to ensure that the plant can operate and experience expected operational transients without unnecessary trips or safeguards actuations.

Part 1 of ISA-S67.04-1994 [3], which is endorsed by Regulatory Guide 1.105, Rev. 3 [4], identifies the following relationships among the safety-related setpoints.

- The limiting trip setpoint (LTSP) is the least conservative value of the nominal trip setpoint that still protects the AL.

- The nominal trip setpoint (NTSP) can be more conservative than the LTSP due to plant conditions or as a compensatory action.

- The actual trip setpoint is known only at the time of measurement, as instrument uncertainty (including drift) will cause the actual trip setpoint to vary over a small range. It is the as-found or as-left value when measured.

Figure 40 provides a graphical relationship between these values, and Fig. 41 shows a hierarchy of control used to avoid tip setpoints.

The choice of a LTSP requires determining the Total Loop Uncertainty (TLU). The TLU represents the expected performance of the instrumentation under any applicable process and environmental conditions. Note that the trip or actuation is only required to mitigate certain postulated events; only the process and environmental conditions that occur during those postulated events need to be considered. The LTSP and NTSP for a trip or actuation on an increasing process would be

$$\text{LTSP} = \text{AL} - \text{TLU}$$
$$\text{NTSP} = \text{AL} - \text{TLU} - \text{Margin} ,$$

where margin is discretionary or may be chosen based on the methodology applied.

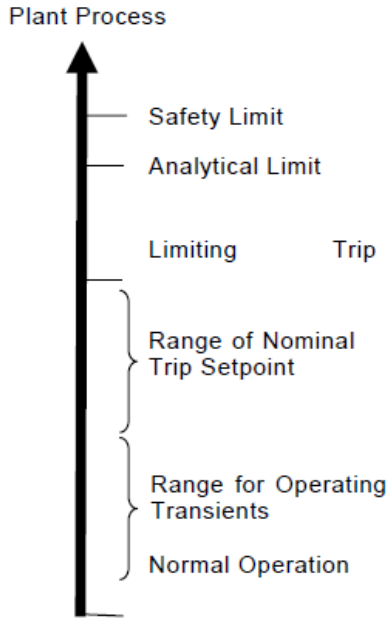


Fig. 40. Nuclear safety-related setpoint relationships. [Source: Part 1 of ISA-S67.04-1994]

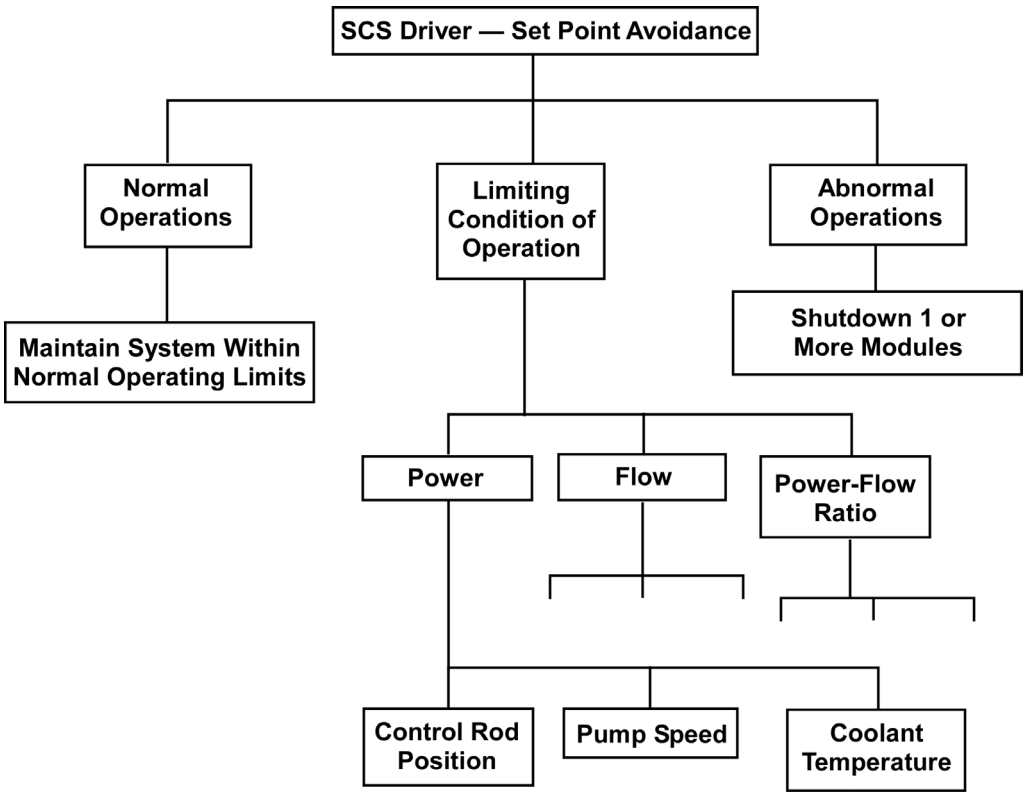


Fig. 41. Hierarchy of control used to avoid trip setpoints.

5.4 SUMMARY—CHAPTER 5

An important function of the supervisory control system is to maintain sufficient margins between plant operating parameters and reactor protection parameters to prevent unnecessary trips. The supervisory control system monitors real-time plant and equipment status and maintains specific knowledge of the action initiation points of the reactor protection system under all operating regimes. The regimes are (1) normal operations, (2) limiting conditions of operations (LCO), and abnormal operations. Transient operations in addition to steady state operations are described in regions of control relative to the current and target states.

Operation anywhere within the homeostatic region is considered normal. The integrated control system employs appropriate feedback control strategies when the system is situated in the homeostatic control region. Should operation be driven into the degraded region, the control objectives become (1) maintain continuous and uninterrupted delivery of principal products of the system if possible; (2) prevent or minimize equipment damage; and (3) avert intervention by the plant safety and protection systems by maneuvering the system away from the envelope inscribed by the safety system. Three types of crises are possible under abnormal operation—stability, viability, and integrity—in increasing severity and inability to return the plant to an operating status.

5.5 REFERENCES – CHAPTER 5

1. R. A. Kisner and G. V. S. Raju, *Automating Large-Scale Power Plant Systems: A Perspective and Philosophy*, ORNL/TM-9500, Oak Ridge National Laboratory (December 1984).
2. General Atomics, *Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor*, DOE-HTGR-86-011, Rev. 5, Vol. 1 (April 1988).

3. Setpoints for Nuclear Safety-Related Instrumentation, *Instrumentation, Systems, and Automation Society (ISA)*, ANSI/ISA-67.04.01-2006 (Approved 16 May 2006).
4. Regulatory Guide 1.105, Rev. 3, *Setpoints for Safety-Related Instrumentation*, U.S. Nuclear Regulatory Commission (December 1999).

6. INFORMATION THEORETIC APPROACH TO ARCHITECTURE

Information is a principal part of most decision-making processes. A reactor operator (RO) in conventional plants makes decisions and acts as a controller that issues commands based upon information about the state of the reactor, plant, and environment. For supervisory control, the same observations can be made, with the supervisory controller using information about the plant to determine control actions, based on predefined rules, to steer the plant to a desired state.

The supervisory control proceeds according a universal paradigm for feedback controllers: First, sensors measure the processes providing information about the state of the plant in the sensing step; this information is processed according to a determined strategy in the decision step; finally, commands are sent (fed back) to actuators to redirect the plant as required in the actuation step. For the supervisory controller's architecture, a group of agents can be imagined that performs these steps of sensing, decision, and actuation. Of interest here is the evaluation of the supervisory controller, its agents, their organization, and performance in the presence of faults. Yet, our interest is more than the mere fault tolerance of the resulting supervisory controller; rather, it is those aspects related to the architecture of the control system, how they affect our knowledge of the state of the plant, and our ability to steer them to a desired state. The challenge is to find ways to evaluate the effect of system architecture on the overall plant performance. Also, we would like to be able to evaluate the advantages of inspection and maintenance programs versus real-time fault-tolerance schemes that use error checking and redundancy to repair the system in real-time.

As the supervisory control system becomes more sophisticated, incorporating logic and high-level decision-making into its processes, we face several challenges: The system itself becomes so complicated that traditional analysis tools are cumbersome to use; the existing methods for evaluating control systems can be lacking; and suitable metrics that relate controller action to controller performance are missing. We should realize that mechanisms for fault tolerance are themselves feedback controllers, but the traditional tools for feedback control are inadequate for evaluating such schemes. This section presents an approach to analyzing controllers that use information-theoretic tools for evaluating their performance.

6.1 INFORMATION AND CONTROL FROM A REACTOR OPERATOR'S PERSPECTIVE

A new method for analyzing control system architectures based on entropy has been developed. The objective of the theory, which is based on the work of Touchette and Lloyd [1] that uses the entropy metric defined by Shannon for information systems, is to estimate, then by evaluating design alternatives, minimize, the entropy of the system.

Consider a multi-unit SMR plant and its heat allocation system, and a RO who must determine which unit delivers steam to a turbine. A RO's task is to actuate a valve that delivers steam from one of two SMR units to the turbine. The valve is set to one of two positions depending upon whether steam is being supplied by Unit 1 or Unit 2. In order to perform this task properly, avoid accidents, and deliver steam to the turbine, the RO must be correctly informed about which unit (1 or 2) is providing steam, and thus receive one bit of information. This can be generalized to more units, as illustrated in Fig. 42. For the case of three units, a three-way valve (three units) requires 2 bits of information, as does a four-way valve (four units); extending this further, an eight-way valve (eight units) requires 3 bits of information. In general, at least $\log_2 N$ bits of information is needed to determine which unit of an N-unit plant is supplying steam.

This logarithmic measure is a natural choice for such information metrics. It can be interpreted as the number of *yes/no* questions needed to determine the state of the plant. As such, it is a function of the number of alternatives of the system considered. More importantly, it is an additive function of that

number in the following sense: Two units with N states each are added together to make a two-unit plant with N^2 states (Cartesian product). This two-unit plant possesses twice the information as one system with N states; it takes $\log_2 N$ bits to determine the state of the first unit, plus $\log_2 N$ bits to determine the state of the second unit.

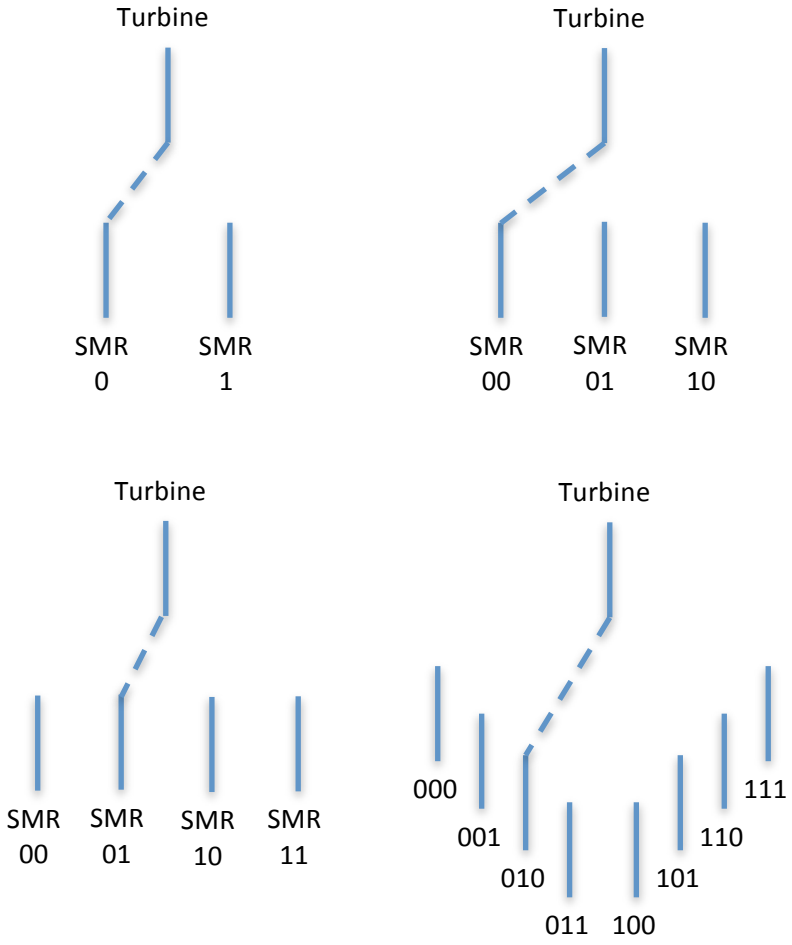


Fig. 42. Multi-unit configurations illustrating the number of bits of information needed to determine which unit supplies steam to the turbine.

Information in this context depends only on the number of alternatives, and not on the meaning of that information. This dependency is important because our definition of information depends only upon its structural characteristics, that is, its number of alternatives and the probability of each alternative occurring. From the perspective of supervisory control, the meaning of the information processed by the supervisory controller plays no role in the supervisory controller's performance. Rather, the pertinent question is "How much information is there about the plant, and how can this information be used to control the plant?"

6.2 INFORMATION, UNCERTAINTY, AND ENTROPY

For an N-unit plant and N-way valve, the amount of information is $\log_2 N$, but this is not the most general way to pose the problem. For example, consider a two-unit plant but where the preference for using unit 1 is greater than unit 2 when, for example, economic dispatch is considered. In this case, the probability of

using steam from unit 1 is greater than unit 2 (in our simple example unit 1 and 2 are operated exclusively), and our simple metric for information is lacking.

The proper metric is the *entropy*, [2], defined as

$$H(X) = -\sum_{x} p(x) \log p(x) ,$$

where X is a random variable and x is a single alternative drawn from the set of all alternatives. Note that the entropy is a function of the probability distribution that describes the random variable X. It does not depend upon the values taken by X. The entropy has the property

$$0 \leq H(X) \leq \log N_X ,$$

where N_X is the number of alternatives for X; thus, it fits our heuristic definition given earlier.

The entropy is zero if the state of X is known perfectly; that is, the probability is one for some state—and necessarily zero for the others. The entropy is maximum if the distribution describing the random variable X is uniform.

$$p(x) = \frac{1}{N_X} \text{ when } H(X) = \log N_X .$$

These two extremes relate to our level of uncertainty about *X*.

- $H(X) = 0$: Complete certainty about the system, that is, no additional information is needed to determine its state.

- $H(X) = \log N_x$: Complete uncertainty about the system. In this case, any one of the states could occur with equal probability (e.g., roll on a die with probability 1/6). As discussed previously, it takes $\log N_X$ questions to determine the system's state.

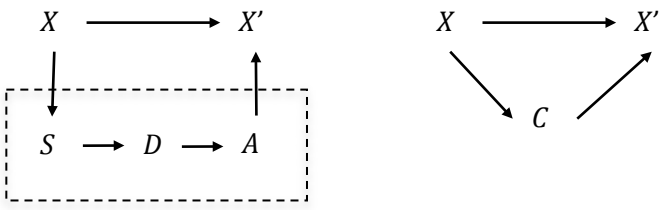
6.3 ENTROPY AND FEEDBACK CONTROL

The transition of the plant from a state *X* to a state *X'* can be described using the Bayesian network.

$$X \longrightarrow X'$$

Such Bayesian networks are probabilistic graphical models that represent random variables and their conditional dependencies. For example, the graph given above could represent the probabilistic relationship between reactor temperature and pressure and safety limit excursions. Alternately, the transition of the plant, under the action of its dynamics, from a current state, *X*, to a future state, *X'*, can be considered. The objective of the supervisory controller is to change favorably the dynamics of the plant. The action of the supervisory controller will be to sense the current state *X* and apply a control input(s) to the plant so that the future state *X'* is the desired state and that this state occurs with high probability. In this condition, the entropy (uncertainty) of the plant is small, as required.

Sensors collect data, and this information is used to determine the state of the plant. Based upon this state, the decision process determines which control action to take, and action is taken to transfer the plant to a new desired state. The transition state can be represented with the following Bayesian networks.



Here the controller *C* on the right is a composite of the sensing, decision, and actuation transitions $S \rightarrow D \rightarrow A$. When the control action is based upon the plant's state, it is so-called feedback (closed-loop) control. However, it should be realized that the sensing step is, in fact, not requisite since decisions can be made without explicit knowledge of the state. For example, regularly scheduled maintenance and repair is often based upon modeled failure rates and not on the actual failure state of the components being replaced. Such control schemes are termed *open-loop* control because they use no knowledge of the plant state.

In the feedback case, the state of the controller, *C*, depends upon the initial state of the plant, *X*. As mentioned previously, for supervisory control and fault tolerance, the objective is to reduce the entropy of the system; that is, given a system with some randomness or uncertainty, the action of control is to shrink the volume of the state space of the system (in a statistical sense), ideally making a single, desired state occur with probability one. This change in entropy is

$$\Delta H = H(X) - H(X'),$$

and depends upon the type of control being used. If the controller is doing its job, this change is positive — the state *X'* has lower entropy than the state X.

In their seminal work, Touchette and Lloyd [1] prove the fundamental relationship

$$\Delta H_{\text{closed}} \leq \Delta H_{\text{open}} + I(X;C),$$

where $I(X;C)$ is the *mutual information* between the state X and controller C and measures the reduction in the uncertainty of the plant's state, X, due to the knowledge of controller C. This inequality shows the following: using information about the state of the plant, one can do better than control methods that do not use such information and the margin of improvement is related to how much the controller "knows" about the plant as measured by the mutual information. This is intuitively pleasing because one would expect use of the information about the plant to be beneficial (if not requisite) for controlling the plant. However, note that this relationship is an inequality and that not all feedback control schemes are necessarily better; in fact, there are lots of ineffective controllers out there. Furthermore, some control schemes do exist that can eliminate any uncertainty about the plant without any knowledge of its state. For example, a reactor trip, which does not necessarily need to know anything about the plant, and hence, is an open-loop scheme, takes the reactor to a hot shutdown state with near certainty. Of course, this simplified example does not meet other necessary objectives, like producing power, which must be considered.

The approach of using information-theoretic tools for analyzing control systems is fairly new. A few examples exist for academic and theoretically interesting problems, but little has been done to apply the techniques to real-world problems, much less those that are energy or nuclear related. Even so, as will be illustrated below, the technique has use for such problems. This is particularly the case since nuclear-related problems already consider scenarios on a probabilistic basis using tools like probabilistic risk assessment (PRA). Although such methods have not explicitly analyzed problems with the information-

theoretic approach presented here, they do evaluate the performance of controllers when evaluating the fault-tolerance of plant control and safety systems. The theory and tools presented in this report can be considered to be an adjunct that provides a well-defined metric of uncertainty to existing tools. These information-theoretic tools are particularly useful when there are a large number of alternatives to consider, and it is not straightforward to evaluate an option based solely on a single probability of occurrence.

6.4 ILLUSTRATIVE EXAMPLES

To demonstrate the methods and its application to nuclear-related problems, two examples are presented that illustrate various aspects of the approach presented above.

1. **ADS fault-tolerance**: The comparison of two requirements for fault-tolerance for an automatic depressurization system (ADS).

2. **Reactor trip system**: The comparison two architectures of a reactor trip system (RTS) using four redundant divisions. The first architecture considers each division to be completely independent; the second includes signal communication between divisions.

6.4.1 ADS Fault Tolerance

The ADS is a safety-related system with two parallel trains that blow down into the suppression pool and is used to reduce the pressure in the primary system to below that of the injection system. A simplified block diagram representation is shown in Fig. 43. The ADS uses pressure relief valves to depressurize the reactor, and block valves are used to prevent an inadvertent blowdown.

The operating conditions are that the power-operated relief valves (PORVs) are normally closed, and the block valves are normally open. Electric power is supplied to the PORVs with division A supplying PORV 1 and division B supplying PORV 2.

The basic failure events and their probabilities are described in Table 6.

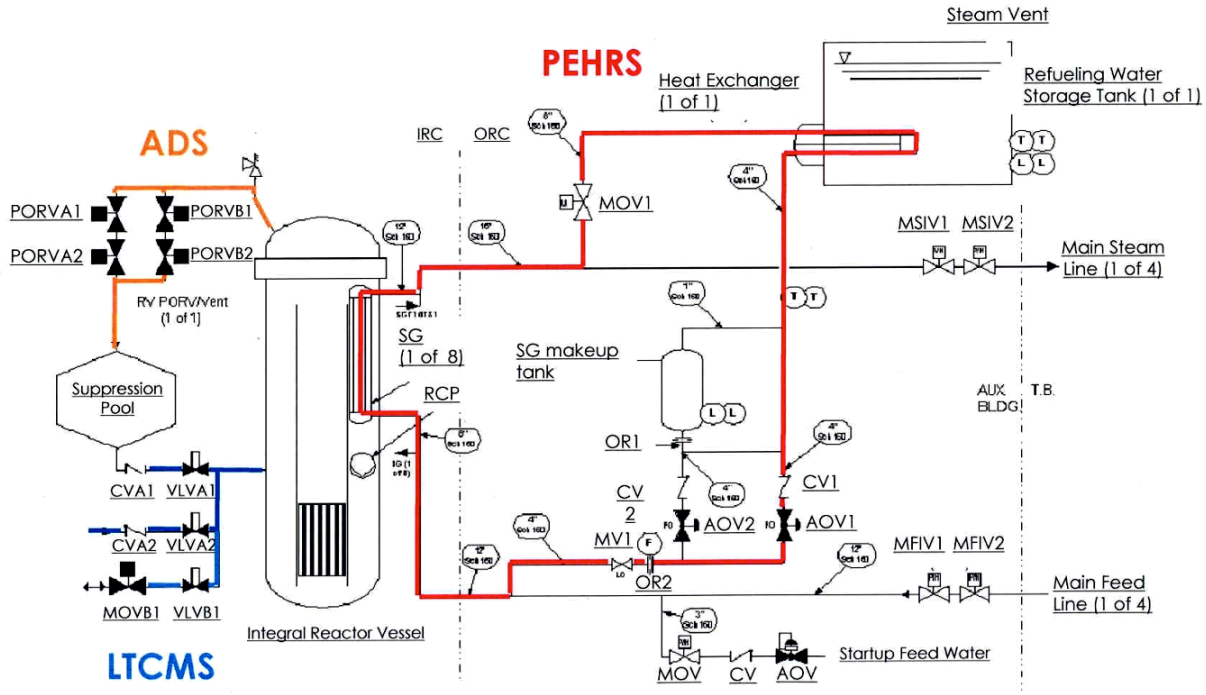


Fig. 43. Reactor schematic showing the ADS.

Table 6. Simplified failure events and associated probabilities for the ADS

Label	Name	Description	Probability of Failure
A	DIV-AB-DC	CCF[a] DivA & B power	6.00×10^{-5}
B	DIV-A-DC	Failure Div A power	6.00×10^{-4}
C	DIV-B-DC	Failure Div B power	6.00×10^{-4}
D	PPR-CCF-XM-OPN2	CCF PORV to open	1.90×10^{-4}
E	PPR-SVR-CC-FO1	PORV 1 fail to open	6.30×10^{-3}
F	PPR-SVR-CC-FO2	PORV 2 fail to open	6.30×10^{-3}
G	PPR-BLK-MOV-TC1	PORV 1 BV closed	4.00×10^{-5}
I	PPR-BLK-MOV-TC1	PORV 2 BV closed	4.00×10^{-5}

[a] CCF: Common-cause failure

Each event, A through I, is a binary state: {OPERATIONAL = 0, FAILURE =1}. The combination of these eight events results in $2^8 = 256$ distinct alternatives.

Eight bits of information are required to determine the state of the system, one *yes/no* question for each failure event, "Is system *A* operational?", and so on. However, due to the small probability of occurrence

of each failure event, the uncertainty is considerably lower than those 8 bits. Because each failure event occurs independently, the entropy of the composite failure is

$$H(X) = H(A) + H(B) + H(C) + H(D) + H(E) + H(F) + H(G) + H(I) = 0.1296 \text{ bit}.$$

This value is somewhat lower than 8 bits but not zero, quantifying the level of uncertainty about the failure state of all of the components. Note that this does not represent the uncertainty of the ADS system itself, which depends upon other criteria.

For example, significance lies in the transition from the component failure state *X* to the ADS failure state *Y*.

$$X \longrightarrow Y,$$

where $Y = \{\text{ADS OPERATIONAL} = 0, \text{ADS FAIL} = 1\}$. To do this transition, consider the failure requirements.

For either train to fail, one of the following must occur: common cause failure of divisions A and B power, failure of the division supplying the train, a common cause failure of either PORV to open, or a failure of the blocking valve closed. Mathematically, this is expressed as

$$\text{Train A FAIL} = A \text{ or } B \text{ or } D \text{ or } E \text{ or } G$$
$$\text{Train B FAIL} = A \text{ or } C \text{ or } D \text{ or } F \text{ or } I$$

For failure of the ADS system, two system options are considered:

1. **ADS 50%:** Failure of the ADS system results from failure of one of the two trains; that is, both trains are required for the ADS to function properly.

$$\text{ADS FAIL} = \text{Train A FAIL or Train B FAIL}$$

2. **ADS 100%:** Failure of the ADS system results from failure of both trains; that is, only one of the two trains is required for the ADS to function properly.

$$\text{ADS FAIL} = \text{Train A FAIL and Train B FAIL}$$

These two scenarios are shown in the event tree in the figures. The probabilities and corresponding ADS failure state were calculated for the two scenarios with the following results:

	ADS 100%	**ADS 50%**
ADS failure probability	2.98×10^{-4}	1.407×10^{-2}
Entropy	3.92×10^{-3} bit	0.1067 bit

As expected, the probability of a failure of the ADS system increases from the ADS 100% case, which requires both trains to fail for the ADS to fail, to the ADS 50% case, which requires only one train to fail for the ADS to fail (Figs. 44 and 45). The entropy tells this story as well. By requiring both trains to be operational our uncertainty about the state of the ADS goes up markedly. This is because to determine the system's true state, information is required about both trains. While the basis for accepting or rejecting one option versus another can be done based solely on the probability of failure of the system, the entropy

provides us with additional criteria, which can be useful if the goal is to develop programs for maintenance and repair, or more relevant to supervisory control, develop real-time fault-tolerance and repair.

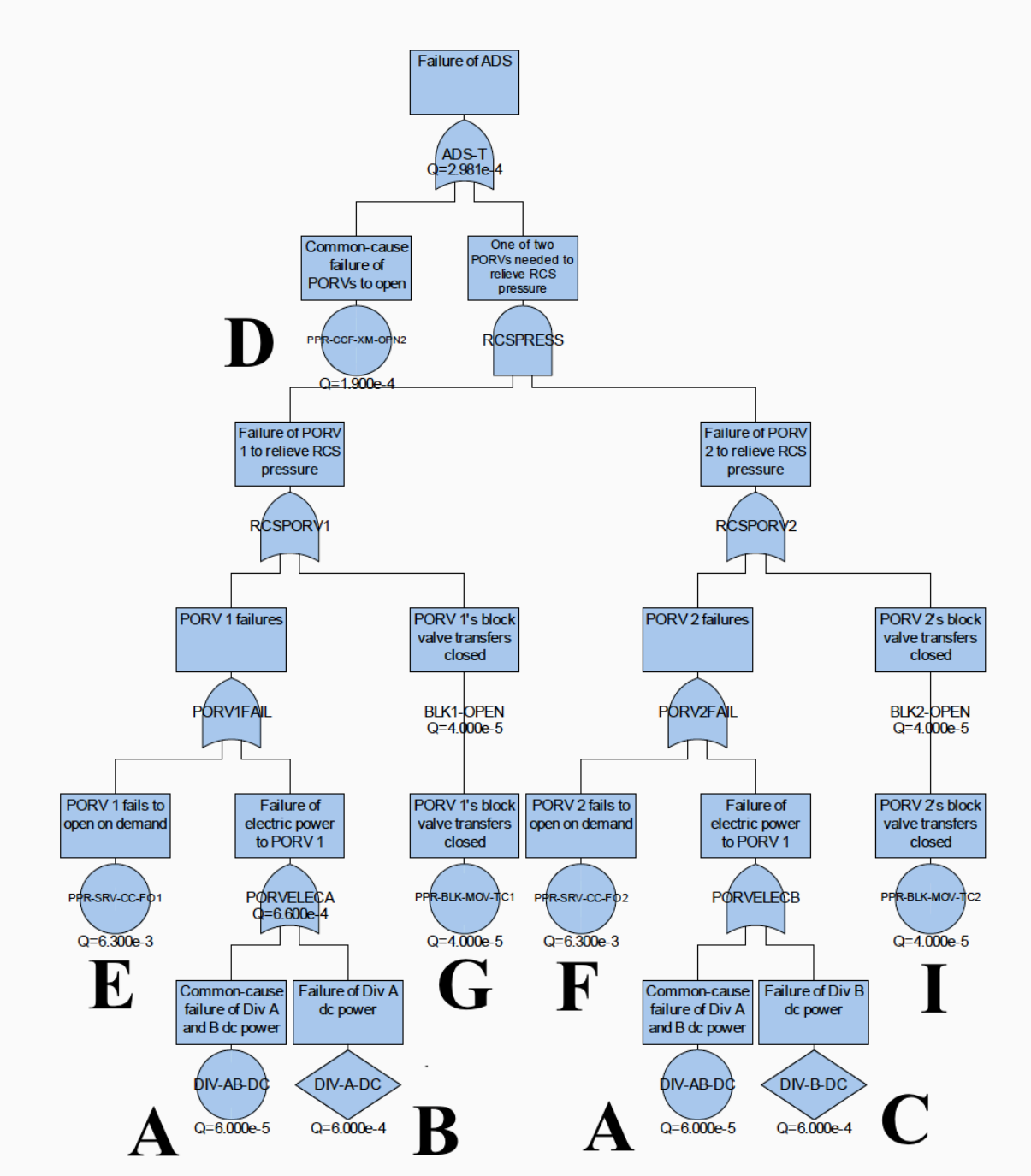


Fig. 44. The event tree for the 50% ADS scenario.

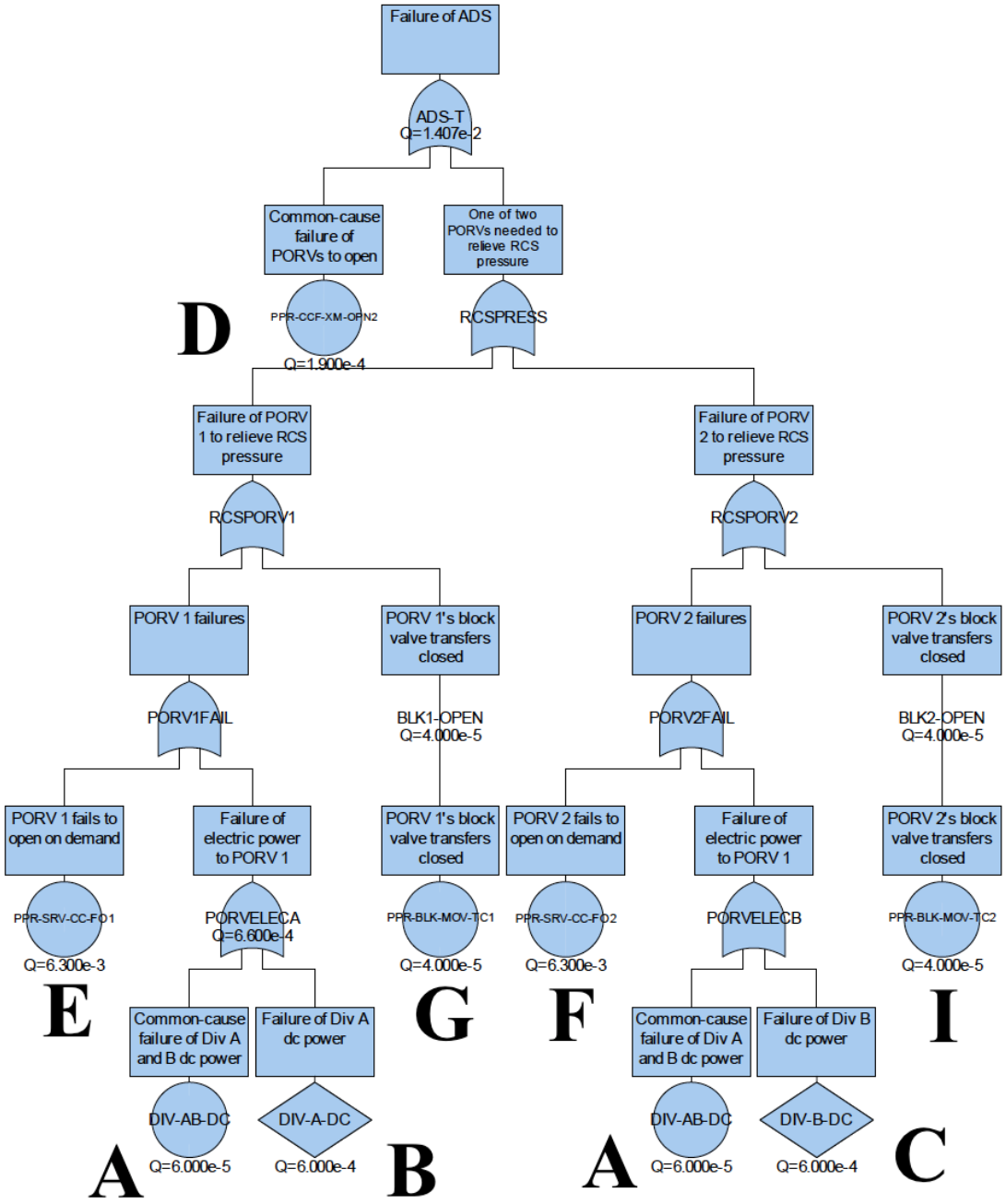


Fig. 45. The event tree for the 100% ADS scenario.

6.4.2 Reactor Trip System

A reactor trip system (RTS) is a safety system. It uses information about the state of the reactor, e.g., temperature above or below a setpoint to initiate a reactor trip. The reactor trip system (RTS) consists of four redundant divisions. Processing of signals is identical in the four divisions. Four redundant measurements of temperature are made. In our model, the sensor signal is binary with COLD and HOT signals, depending upon if the temperature is above or below a setpoint. In hardware, the sensor measurements are compared to the setpoint in digital trip module (DTM) yielding a binary signal. The

binary signal is then processed by a voter logic unit (VLU). The VLU provide for bypass of trip functions to accommodate period tests and maintenance. Bypassing two or more divisions is not permitted.

Two architectures for the VLU are considered.

1. The VLU in normal operations sends the input from the DTM of its division to the SLU, as represented in Fig. 46.

2. The VLU receives input from the DTMs of all four divisions. The output of the VLU uses 2-out-of-4 logic, as shown in Fig. 47.

The output of the VLU is a binary trip signal. The output from all four VLUs are then processed by the safety system logic unit (SSL) using a 2-out-of-4 voting scheme yielding a reactor trip signal. This reactor trip signal is the random variable C.

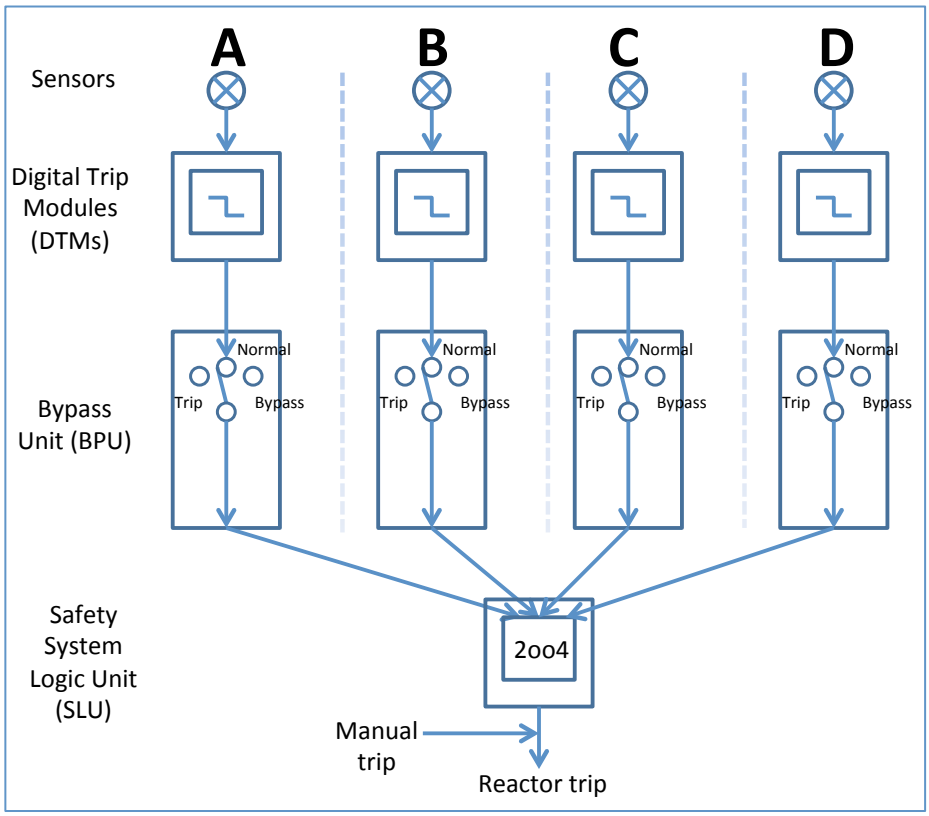


Fig. 46. Schematic of the reactor trip system with the Simplex architecture.

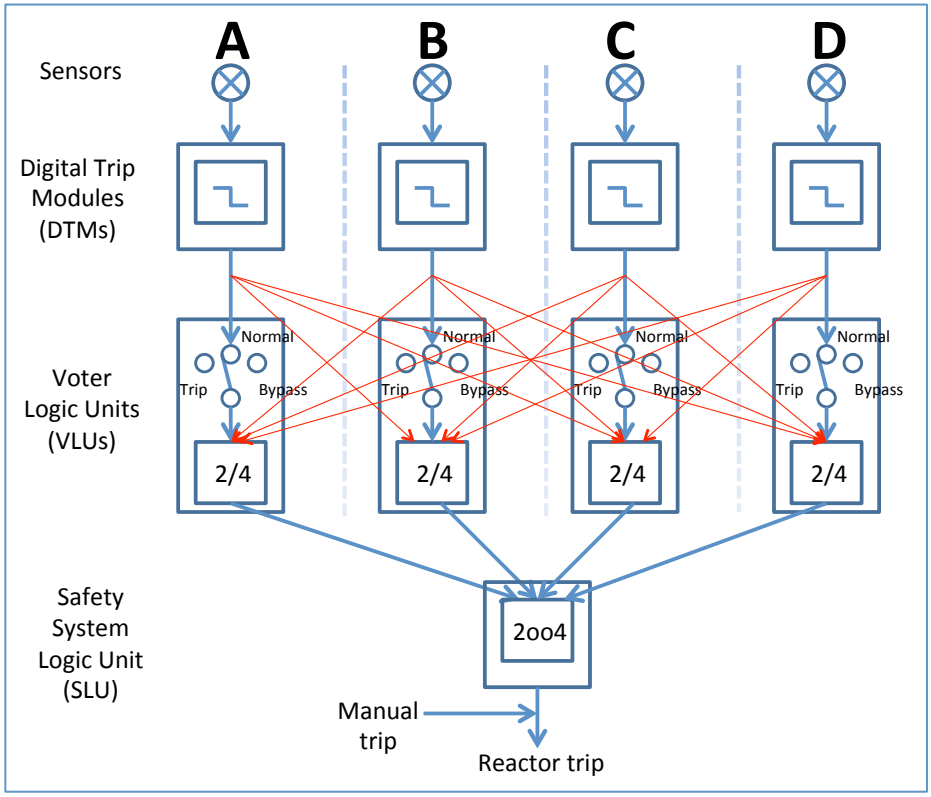


Fig. 47. Schematic of the reactor trip system with the N-modular redundant architecture.

Table 7 shows the modeled components in the RTS, the model variables, and their state space. As can be seen, only binary state-space representation is used to simplify the demonstration. Failure probabilities for each component are listed in Table 8.

Table 7. Probability state space for the RTS components

Component	Variable	Possible States
Reactor Temperature	X	{COLD = 0, HOT = 1}
Sensor	S	{COLD = 0, HOT = 1}
Digital Trip Module (DTM)	D	{BELOW = 0, ABOVE = 1}
Voter Logic Unit (VLU)	V	{NO TRIP = 0, TRIP = 1}
Safety Logic Unit (SLU)	C	{NO TRIP = 0, TRIP = 1}
Failure	F	{OK = 0, FAIL = 1}

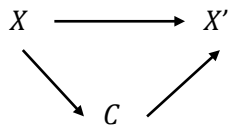
Table 8. Probabilities of failure events for the RTS components

Component	Failure Event	Description	Probability
Sensor	F_S	sensor failure	2.00×10^{-4}
Digital Trip Module (DTM)	F_D	DTM failure	9.00×10^{-4}
Voter Logic Unit (VLU)	F_V	VLU failure	6.24×10^{-4}
Safety Logic Unit (SLU)	F_C	SLU failure	8.00×10^{-5}

It is assumed that when a unit fails, it fails in a manner that would be unfavorable for safety; that is, sensor outputs a **LOW** signal, and the DTM, VLU, and SLU output a **NO TRIP** signal.

6.4.2.1 Control Scheme

The RTS state transition can be represented with the Bayesian network as follows:



where the reactor state, X, is its temperature, which for the analysis can be considered to be HOT or COLD. These designations do not reflect operating states of the reactor, but rather label of the general region its temperature is in.

The entropy of the temperature state depends upon the probability in each of these alternatives. It is straightforward to show that the maximum entropy of the temperature state is 1 bit if

$$p_{\text{HOT}} = p_{\text{COLD}} = 1/2$$

In reality, the probability of the temperature exceeding its setpoint, which would ideally result in a trip, is lower, assume $p_{\text{HOT}} = 0.1$. The entropy associated with the reactor temperature before any control action is calculated as

$$H(X) = 0.46900\ bit \quad \text{(before control)}$$

The control signal C is a trip signal to the reactor: **NO TRIP** or **TRIP**. The future reactor state X' is the temperature of the reactor sometime after the trip signal is sent (or not). The transition of the reactor from state X to X' depends naturally on the control signal.

- If $c = 0$—i.e., **NO TRIP**—then the reactor in a high temperature state, $x = 1$, stays in a high temperature state, $x' = 1$; similary a reactor in a low temperature state, $x = 0$, stays in a low temperature state $x' = 0$.

- If $c = 1$—i.e., **TRIP**, then the reactor is always returned to low temperature state regardless of the state it begins in.

This second control dependency is unique in that it takes the reactor to a single alternative, low temperature, with probability one. Thus if $c = 1$—i.e., **TRIP**—then the entropy is calculated to be

$$H(X) = 0\ bit.$$

This is as required since the objective of the RTS is to return the reactor to a hot shutdown state and remove uncertainty about its state. It should be pointed out that the assumption that this state is achieved with probability one is optimistic, and assumes all necessary reactor safety systems work perfectly. In this study, our interest is in the architecture and communication of the RTS itself, so these assumptions will be sufficient for now.

6.4.2.2 Comparison of Architectures

The Bayesian networks shown in Figs. 48 and 49 describe the conditional dependencies of control signal on the temperature state X and the failure states for each of the components. In both cases, the network can be reduced to a single conditional dependency relating X and C. This conditional dependency describes the control law in a statistical sense, and is described by the conditional probability matrix.

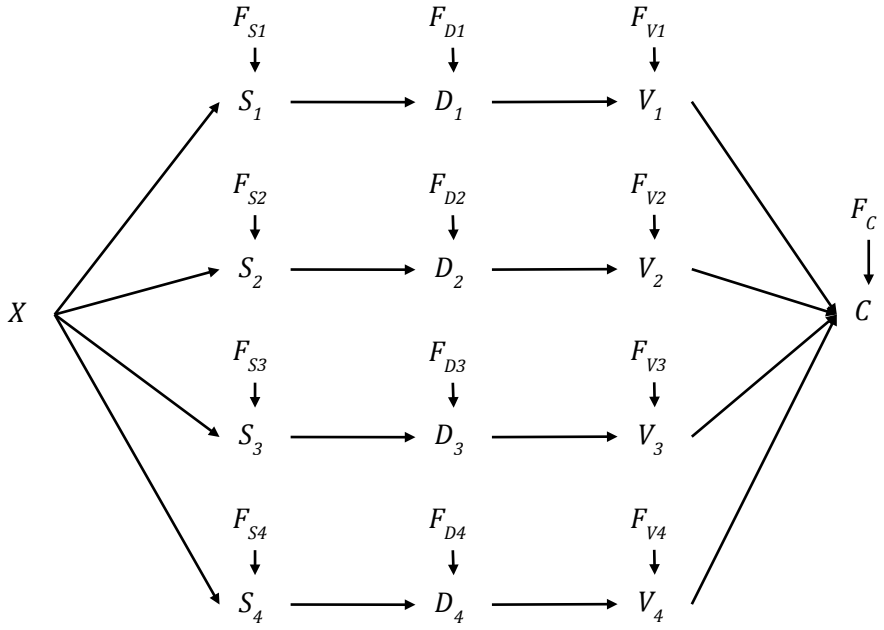


Fig. 48. The Bayesian network for the RTS with no cross communication.

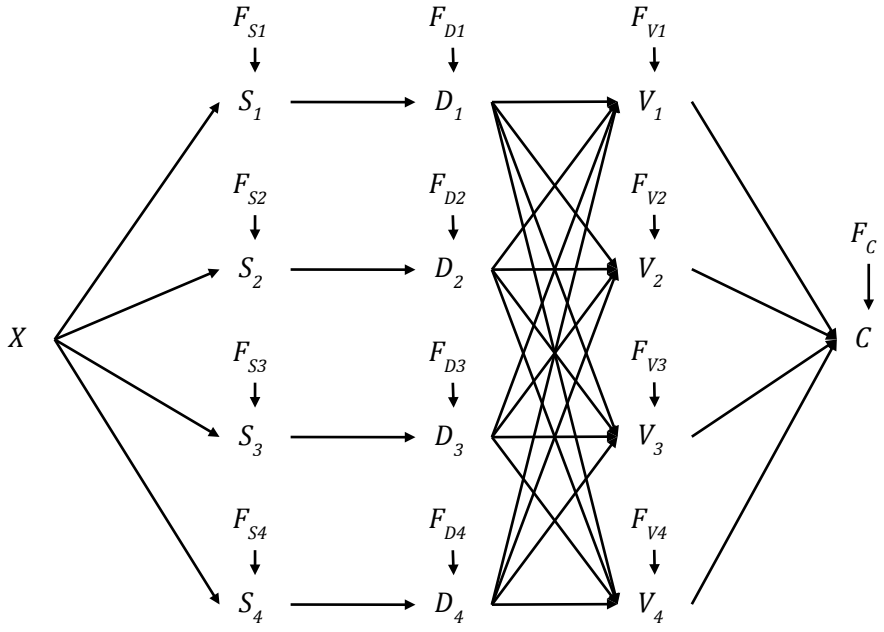


Fig. 49. The Bayesian network for the RTS with cross communication.

The fact that the conditional probability matrix is nearly the same for both architectures is likely due to the symmetry of the problem.

It should be noted that if the reactor temperature is in a COLD state, the RTS will not trip with probability one. This is a result of the fact that all failures of the components result in conditions that are unfavorable from a safety perspective; that is, all give a **NO TRIP** condition. This is, in fact, unrealistic. A more realistic scenario would be if a failed component gave either a **TRIP** or **NO TRIP** signal with equal probability.

The above conditional probabilities can be combined with the dependency of X' on X and C to yield the entropy of the future state. The results are nearly identical for the two architectures with

$$H(X') = 1.4700\times10^{-4} \text{ bit.}$$

with the resulting change in entropy

$$\Delta H = H(X) - H(X') = 0.46885.$$

As expected the RTS eliminates nearly all of the uncertainty in the reactor state. If the two architectures are compared based on these results, the conclusion is that they are effectively equal, and that there may be no benefit to the added complexity of including additional communication channels.

A different picture results when one of the VLUs is bypassed (assume unit 1). In this case, the resulting conditional probabilities are as follows:

	$x = 0$	$x = 1$
$c = 0$	1	8.8897×10^{-5}
$c = 1$	0	0.99991

Independent divisions with bypass of VLU 1

	$x = 0$	$x = 1$
$c = 0$	1	8.1173×10^{-5}
$c = 1$	0	0.99992

Cross-communication with bypass of VLU 1

For this case the two architectures do prove different with the cross-communication architecture yielding a lower probability of a **NO TRIP** signal when one is required.

The entropy and entropy change for the two architectures is calculated as follows:

	Independent divisions	**Cross-communication**
$H(X')$	1.6199×10^{-4} bit	1.4898×10^{-4} bit
$\Delta H = H(X) - H(X')$	0.46885 bit	0.46885 bit

The total entropy change for the two architectures is nearly equal. The cross-communication architecture does result in marginally lower uncertainty in the final state of the reactor by improving on $H(X')$ by an additional $0.1301 \times 10^{-4}\ bit$. Whether this improvement is warranted or necessary depends upon externally imposed criteria. Establishing such criteria is a subject of future research.

6.4.2.3 Discussion on Analyses

There are several advantages to the overall approach of using information-theoretic metrics to evaluate system randomness. First, the approach is probability based, and thus lends itself to other fault-tolerance techniques and methods for evaluating risk, like PRA. What distinguishes this approach from others it that there is a specific metric, the entropy, for evaluating the uncertainty of the controlled system. Also, a fault-tolerance technique can be compared with other approaches, and its optimality assessed. These features allow for the analysis of trade-offs in the design of fault-tolerance systems.

While the examples given here are drawn directly from fault-tolerance analysis, the technique can be applied to any probabilistic treatment of system behavior: for example, stochastic dynamics, Monte Carlo simulations, random dispatch requests, or randomized RO responses. Furthermore, because entropy is an uncertainty metric on an entire probability distribution, large spaces of alternatives can be evaluated. Thus, it can be used to evaluate scenarios where the probability of being in multiple states is needed; for example, the consideration of limits where there is different limit safety.

Finally, while entropy provides a single useful engineering metric for randomness, it can hide details of a probability distribution that could be useful for evaluation and decision-making. Furthermore, it is not yet apparent that a comparison cost/benefit between controllers in terms of dollars per bit, say, is meaningful or appropriate. Also, it can be desirable to evaluate the estimated magnitude of a final state in terms of severity or risk, and it is not clear how the tools presented here can be used in such situations. Each of these issues is a further topic of research.

6.5 SUMMARY—CHAPTER 6

A new method for analyzing control system architectures based on entropy has been developed. The theory is based on the work of Touchette and Lloyd that uses the entropy metric defined by Shannon for information systems. Because information is a principal part of the supervisory control function, *information entropy* can be used as a measure of the uncertainty in that information and hence the decision-making process. The entropy method may be used both in the design of supervisory control architecture as well as for real-time decision-making.

The method is developed and applied to two examples: (1) ADS fault tolerance and (2) reactor trip system. The results showed that the entropy metric correlated well with PRA based analyses for the first example.

6.6 REFERENCES – CHAPTER 6

1. H. Touchette and S. Lloyd, “Information-theoretic approach to the study of control systems,” *Physica A*, **331**, pp. 140–172 (2004).
2. C. E. Shannon, “A Mathematical Theory of Communication,” The Bell System Technical Journal, 27, pp. 379–423 (Jul. 1948).

7. CYBER SECURITY CONSIDERATIONS FOR SUPERVISORY CONTROL ARCHITECTURE

Instrumentation and Controls Infrastructure (ICI) of a generic Small Modular Reactor (SMR) consists of diverse systems: Instrumentation and Control System (ICS), Data Display and processing System (DDS), and Operation and Control Centers System (OCS). Each of these systems consists of a number of networked components, such as instrumentation and control devices and/or computing servers and end stations, to support monitoring and control operations. Security considerations in designing a cyber infrastructure to support ICI operations are identified, including overall threat space and potential threat vectors. Different cyber zones and two separate networks that underpin ICI are likewise identified, and possible ICI configurations and interconnections are determined by threat space and customized based on threat vectors. In particular, the network for ICS is described in greater detail in terms of physically diverse and redundant network connections and servers, and the network for DDS and OCS in terms of overall design and architecture. Two configurations that address two different threat vectors are described:

(i) two networks for instrumentation and control, and operations and IT services, that are physically separate and are operated and managed separately, and

(ii) two networks for instrumentation and control, and operations and IT services, that are interconnected but through strict firewalls.

These initial designs and perspectives, however, must be further refined by taking into account the details of the components.

In addition to network security considerations, the control system itself can be designed for detection of and resilience to cyber attacks. While network security measures increase the required effort to successfully penetrate the control system, they provide little protection to the system operation once an attacker has gained access. Deploying cyber-attack-resilient control system algorithms will make it more difficult for an attacker to cause damage or disrupt normal operation in the event network security measures are bypassed.

7.1 BACKGROUND

The ICI of a generic SMR, based on Chapter 7 of the AP1000 Design Control Document, is shown in Fig. 50. While there are significant variations in the possible designs and layouts of SMRs, and their versions are still evolving, this AP1000 ICI contains the essential elements and overall generic design to identify the underlying cyber considerations and bound the options for the needed cyber infrastructures.

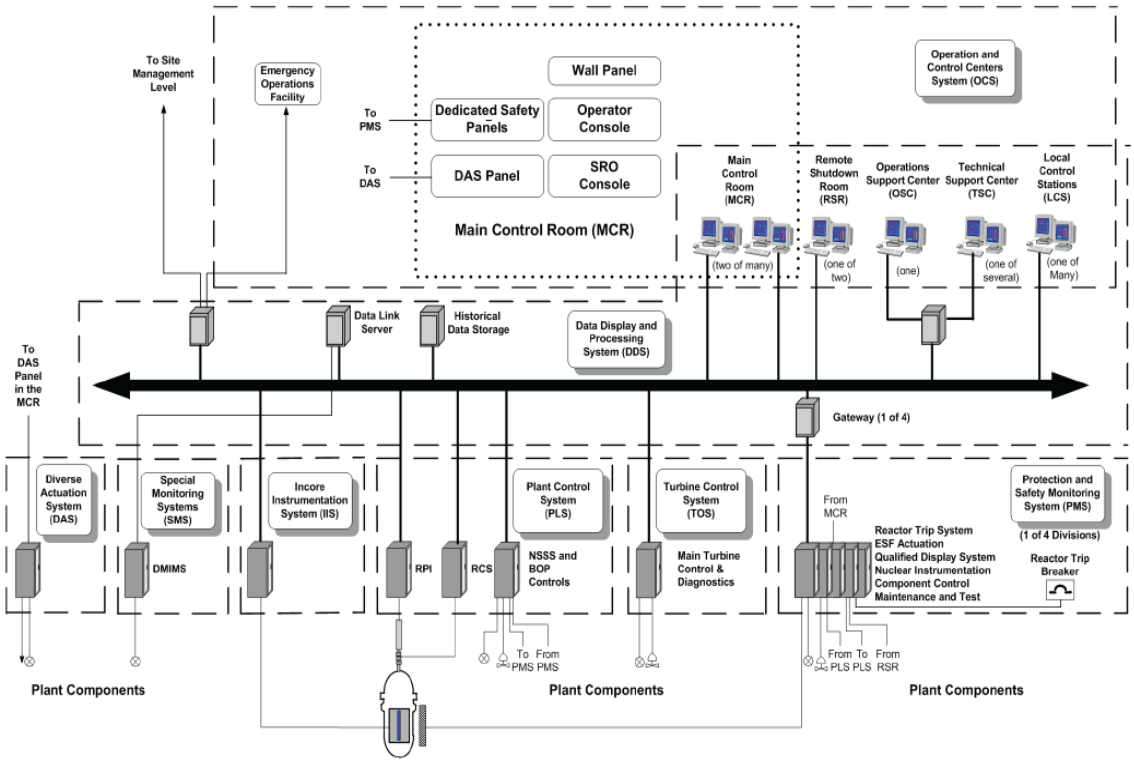


Fig. 50. SMR instrumentation and controls infrastructure layout based on AP1000.

Based on the plant ICI layout, there are three main systems that must be considered from a cyber infrastructure perspective.

1. The *Instrumentation and Control System* (ICS) is composed of diverse actuation, special monitoring, in-core instrumentation, plant control, turbine control, and protection and safety monitoring systems to provide monitoring and control capabilities.

2. The *Data Display and processing System* (DDS) is composed of computing systems that monitor ICS components, process the senor data and present it to operations, and support mechanisms to implement control commands from operations.

3. The *Operation and Control Centers System* (OCS) interfaces with the DDS to implement the monitoring and control capabilities for the Main Control Room (MCR), and also to support the operations, technical support, local controls, and remote shutdown capabilities.

The cyber components of ICI, including computers and network devices, and the interconnection links provide the interoperability within the components of these systems and also between the systems themselves. In general, these systems are characterized by different types of cyber vulnerability considerations, and thus require different types of cyber capabilities. Furthermore, threats can propagate from one system to the other via these networks, and hence such propagation mechanisms must be suitably contained. Based on the plant ICI layout, three cyber zones can be identified and associated with different SMR parts, including plant components, operations and control centers, main control room, remote shutdown room, and others. These cyber zones require different levels and types of cyber defenses and may have to be separated entirely at the physical level or protected from each other using firewall-based diode filters. Consequently, they require different levels of cyber security measures and defenses in

terms of devices, configurations, and concept of operations (CONOPS) that specify software and hardware upgrades and connectivity within local networks and to external networks including the Internet (if needed). Attention is focused on developing the overall cyber security architecture for SMRs, which is responsive to the underlying threat space and the estimated threat vectors described in the next section. Determination of threat vector components, such as precise likelihood estimates of certain cyber attacks, requires threat posture information, which involves certain non-technical information, which is beyond the scope of this report.

Different cyber zones and two different networks are identified in Section 7.2. The overall threat space and vectors are briefly described in Section 7.3, and the instrumentation and control network is discussed in Section 7.4. Section 7.5 addresses the operations network, and Section 7.6 describes interconnection options for establishing and operating both networks. Section 7.7 discusses anomaly detection methods that utilized the deterministic nature of the underlying physical system, and Section 7.8 describes cyber-attack-resilient control system design. Finally, in Section 7.9 provides some conclusions.

7.2 CYBER ZONES AND SEPARATE NETWORKS

Based on the ICI shown in Fig. 50, two different types of networks can be identified to support the cyber operations: (1) Instrumentation and Control System Network (ICSN), and (2) Operations and Control Centers System Network (OCSN).

Instrumentation and Control System Network (ICSN)

The ICSN supports the actuation, monitoring, instrumentation, plant control, turbine control, and protection and safety monitoring component systems. Robust and resilient connectivity to these systems is required to ensure both monitoring and control operations of these component systems. This is a special-purpose local-area network that connects the monitoring and control operations and is designed specifically based on the network interfaces of these component systems. Most of them are expected to be IP enabled but are expected to operate under limited connectivity environments. In particular, these systems are not expected to incorporate cyber measures and defense capabilities needed to operate under Internet environments. Indeed, it is essential to shield them from exposure to potential threats that might originate from the Internet.

Operation and Control Centers System Network (OCSN)

The OCSN connects the main control room computers to those in other operations and control centers. This network mainly consists of servers and user workstations and resembles corporate IT networks. Some part of this network may be connected externally such as connection to a remote shutdown facility, NRC remote site connection, IT operations connection to the Internet for software upgrades, and other possible connections to the Internet. This network might support some workstations with email and instant messenger services to a remote corporate office, if applicable, and others with web browsers.

Based on the plant ICI layout, two cyber zones are identified and associated with different parts, including plant components, operations and control centers, main control room, remote shutdown room, and others. These cyber zones require different levels of cyber defenses and may have to be separated entirely at the physical level or protected from each other using firewall-based diode filters. An overall cyber security architecture for SMRs that is responsive to the estimated threat vectors must be developed. Initial options include a physically separate network that connects plant instrumentation and control with main operations control and a separate cyber infrastructure for operations centers and other external connections, as shown conceptually in Fig. 51. The network and infrastructure may be kept separate or

connected through a firewall, but in either case, further investigation will be have to be conducted, as discussed in the next sections.

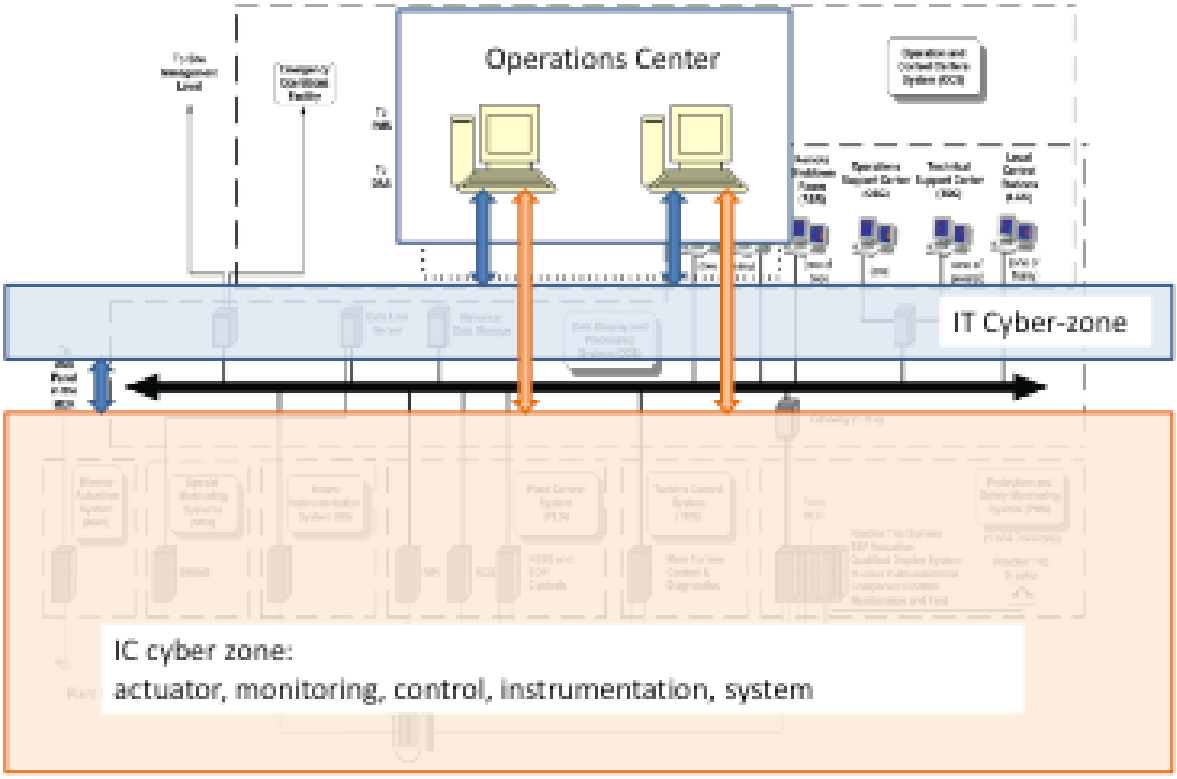


Fig. 51. IT and IC cyber zones.

The details of which option to adopt and the underlying details depend on both the overall threat space and the likelihood of various threats, specified as a threat vector. The corresponding options for cyber zones, their layers of cyber defenses, and their interactions must be taken into account in developing and analyzing the cyber infrastructure.

7.3 THREAT SPACE AND VECTORS

The potential threat space of SMRs is identified to include the following.

(i) *Network Attacks*: Attacks can be launched from external network connections, which include worms, malicious codes, and other target attacks on hosts, servers, routers, switches, instrument monitoring systems, and control systems. For SMRs, particularly important are attacks that spoof monitored variables by either masking the real attacks or creating false alarms that may lead to unnecessary shutdowns. Also conceivable are variations of Stuxnet-type attacks that target the turbine control system. Vulnerabilities of this type can be mitigated to a certain level by isolating parts of the SMR network from external network connections.

(ii) *Non-Network Software Attacks*: Even when no external connections exist, Stuxnet-style attacks can propagate via software upgrades via CDs, USB drives, and similar means. While the means of propagation are different, the class of these attacks could encompass several network attacks.

Vulnerabilities of this type can be mitigated to a certain level by streamlining and strictly controlling the software installation and update processes.

(iii) *Hardware/Firmware Attacks*: Hardware/firmware attacks could be launched using embedded trojans inserted into hardware devices. Such malicious codes can be introduced during the supply chain, when these units are produced. These types of attacks have been historically observed in network devices, and such risks can only be reduced by using hardware components that were produced under strict supply chain controls. It is important to manage the supply chain of various computing and network devices both during the initial designs as well are during subsequent replacements and upgrades.

The threat vector estimation corresponds to assigning likelihood estimates to different threats, and identifying a priority list so that a suitable cyber infrastructure option can be identified. While the threat space could be quite extensive, not all threats are equally likely. Indeed, attackers can range from an individual hacker who utilizes tools available on the Internet to well-financed organizations to state-sponsored cyber offenses. However, is it important to keep up to date with the evolving threat space and vectors, and maintain an appropriate cyber security posture.

7.4 INSTRUMENTATION AND CONTROL NETWORK

A dedicated network connects the monitoring center to various monitoring, actuation, control, and instrumentation systems. Two separate IC server physical locations are deployed, and both are connected to a command center via thin-clients.

a. Software maintenance and upgrades: Internet-based upgrades
b. Hardware maintenance and supply chain management

7.4.1 Thin-Client IC Network

IC network is supported by physically separated server systems that serve remote thin-clients. The physical access to the server locations is strictly limited to authorized personnel only with established procedures for system installations and upgrades in place, including software and hardware upgrades. All monitoring, actuation, control, and instrumentation systems are connected to each server via two physically separate, redundant connections, as shown in Fig. 52.

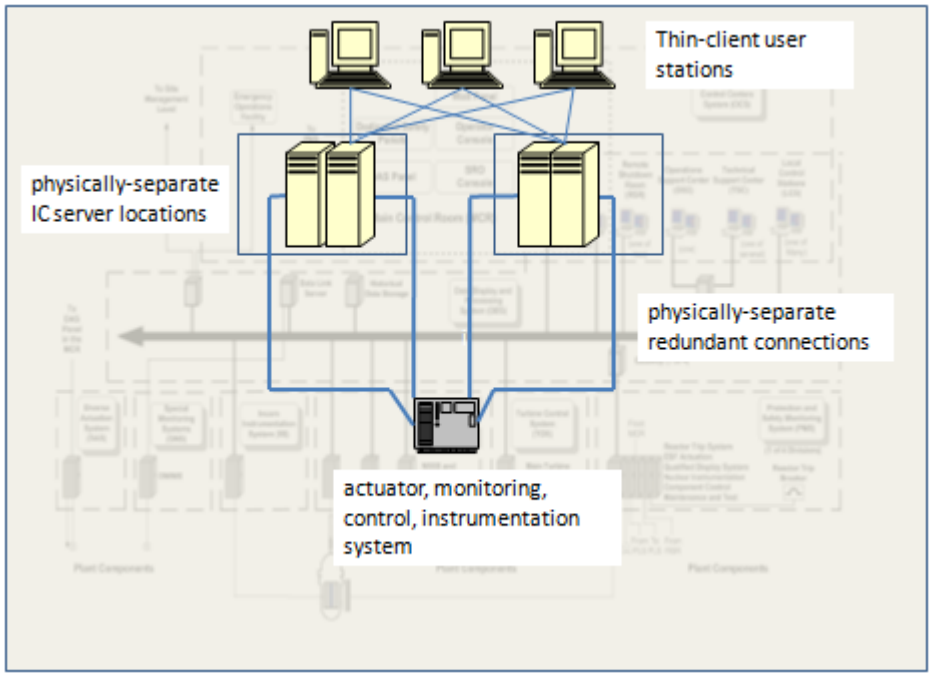


Fig. 52. Thin-client instrumentation and control network.

7.5 OPERATIONS NETWORK

The OCSN is composed of computing systems, including servers and user workstations, and network devices, including switches and router, which have to be designed and maintained to achieve the security posture that matches the threat vector. A practical, cost-effective approach is to deploy COTS devices for both computing and networking components, which requires careful selection of not only the components but also procedures for maintenance and upgrades.

a. *Software maintenance and upgrades*: COTS software, such as operating systems and web browsers, requires patches and upgrades, and currently Internet-based upgrades are the most commonly utilized mechanisms. The usual implementation of this mechanism not only requires Internet connection but often requires higher account privileges. Such practice is considered less secure, and a more effective method is to establish secure zone behind the firewall to capture the updates and install them on a local server that updates the components without maintaining a live Internet connection.

b. *Hardware maintenance and supply chain management*: The components systems must be either procured through trusted supply chains and/or configured to strictly monitor and limit their functionality to well-specified, known behaviors.

c. *External Connections*: External Internet connections must be through a strict firewall with services limited to the essential ones; in particular, by default all service must be filtered out at the firewall and only the essential, well-specified ones must be enabled. All connections to remote control locations and a regulatory remote site (if needed) may be encrypted using point-to-point end devices and may be implemented using physically diverse redundant paths.

7.6 ICSN AND OCSN INTERCONNECTIONS

The interconnections between ICSN and OCSN depend on the precise threat vector, the major consideration being Internet-based Stuxnet-style attacks being able to penetrate ICSN from OCSN. The

most conservative approach is to operate two physically separated networks with no connections between them, as shown in Fig. 53. This configuration requires two separate terminals in the Management Control System (MCS) and Operations on connected to ICSN and the other OCSN; furthermore, the thin-client version of the ICSN terminal reduces potential accidental *spill-over* connections, such as plugging in the OCSN workstation into the ICSN. However, this option represents significant additional cost since two separate networks have to be built and maintained.

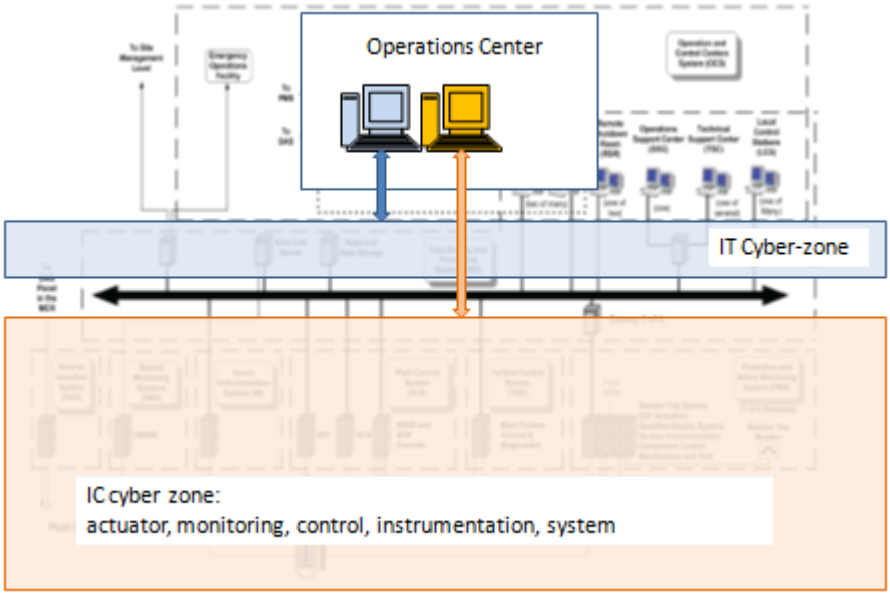


Fig. 53. Physically separated ICSN and OCSN.

In terms of infrastructure and operations costs, the simplest approach is to connect all components into a single IP network such that ICSN and OCSN are separated by physically diverse, redundant firewalls, as shown in Fig. 54. It is important to locate the firewall routers under two separate physical-plant facilities such that a single power failure does not disconnect the ICSN. A strict firewall rule may be configured so that the firewall acts as diode from ICNS to OCSN, except very specific control messages are enabled from OCSN to ICNS. Those conditions in which firewalls can be compromised or misconfigured must be analyzed in detail and accounted for.

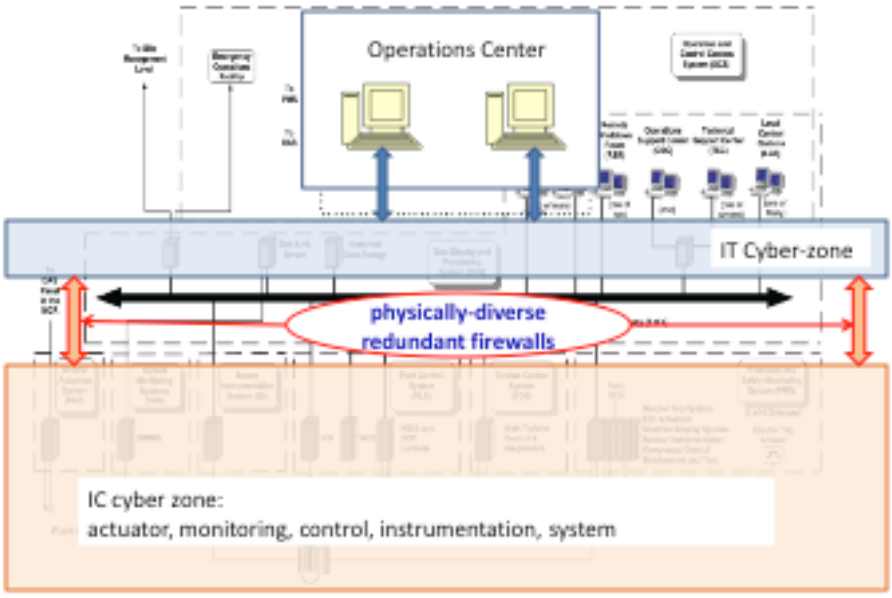


Fig. 54. ICSN and OCSN connected by physically diverse redundant firewalls.

7.7 ANOMALY DETECTION

The deterministic nature of the underlying physical system provides new opportunities for anomaly detection unavailable to the stochastic methods used in network theory, although many of the techniques are similar, and in some instances, stochastic methods are necessary. Control systems experience many different types of anomalies during normal operation from sensor failures to operator error. The most recent category added to this list is cyber-attacks. In most cases, anomalies look the same to the closed-loop dynamics of the control system with the important exception of the potential for active deception efforts by a cyber-attacker.

The most important aspect of anomaly detection is the development of models that capture non-anomalous behavior. These models fall into two categories for control systems: (1) models of the operator commands during normal operation cycles and fault scenarios and (2) models of the closed-loop dynamics of the interaction between the physical system and the controller.

The first potential attack type by a cyber-intruder is the manipulation of reference commands. This attack vector is the most likely one used by unsophisticated adversaries who do not have a high level of knowledge about control system operation. During normal operation, most control systems go through a start-up → normal operation → shutdown cycle. Generally, the sequence of commands to perform these operations is consistent and temporally related. The other primary operating conditions are fault scenarios. These are also governed by predefined safety procedures that are either performed automatically by the control system or manually performed.

Two techniques for developing temporally related models of the stochastic behavior during operation and fault scenarios are Hidden Markov models and Bayesian inference.

Hidden Markov models employ a sequence of states in which the only observable output is the state sequence. This output is then used to estimate the state transition probabilities, which can be used to determine the likelihood that a command is anomalous. Applied to control system operation, the sequence of commands during start-up, normal operation, and shutdown is the observed output. For example, if

during a start-up procedure a feedwater pump is always turned on before a boiler is started, the model will estimate a high probability for this particular state transition. After the model has been trained using operational data, any command sequence that does not fall into the normal operating regime will give a low probability, which can be used to flag attacks or operator error.

Bayesian inference is a similar stochastic method that can be used to predict the likelihood of a sequence of data. It is particularly suited to online updating of the probability distributions.

More sophisticated subtle attacks will modify the actuator inputs, sensor outputs, and controller parameters. To detect attacks of this nature, deterministic models of normal closed-loop dynamics are needed. System identification techniques, both online and offline, are commonly used to develop dynamic system models that are then used to design the controller. These techniques can also be used in anomaly detection including sensor and actuator failure and cyber-attack. These same models can also be used to identify when an actuator signal, sensor signal, or control parameter has been modified by an attacker because the input/output relationship will no longer hold unless the attacker also has an exact model of the system dynamics and can manipulate both input and output signals. This vulnerability can be mitigated by analyzing the system noise, which is difficult to emulate, and by injecting small-amplitude actuator signals that cannot be known a priori by the attacker and looking for their signature in the output.

The estimated likelihood that an attack is occurring and determining the signals that an attacker is manipulating is critical for rejecting the effects of the attack.

7.8 CYBER-RESILIENT CONTROL SYSTEMS

A control system is designed to reject disturbances to the physical system to allow more precise control. This disturbance rejection relies on a number of assumptions that are no longer valid in the case of a cyber-attack. It can be shown that standard linear feedback systems cannot reject manipulations due to a cyber-attack [1]. This leads to the conclusion that cyber-resilience requires additional features beyond just a feedback loop.

Research is ongoing to develop inherent resilience within the control system by new theories and techniques. One area of research is to use fault-tolerant control techniques in conjunction with the anomaly detection methods described in Section 7. Modern fault-tolerant control includes an additional bank of non-linear Kalman filters that is used to estimate sensor and actuator failures or attacks. The control system is then dynamically reconfigured to remain stable without using the compromised sensors and actuators [2]. However, this requires the system to be over-actuated and over-observed, and this is not the case for some simple control loops. Determining sufficient amounts of over-actuation and over-observation is an open problem.

Another area of research is to employ a second self-programming controller that will take over operation if the primary controller has been compromised by an attack. This approach will allow operation for a limited amount of time until the system can be safely shut down or control of the primary controller is regained. The secondary controller has to be self-programming to prevent an attacker from compromising its functionality too. There are a number of challenges to developing the secondary controller. The necessary online system identification algorithms need to be robust and extend to a large spectrum of systems. Command emulation can be subtly manipulated by an attacker. Closed loop control for portions of the system may be compromised. All these factors contribute to the time limit that the secondary controller can maintain operation without intervention.

7.9 SUMMARY—CHAPTER 7

The cyber infrastructure for a small modular reactor requires a blend of defenses that combines instrumentation and control networks and ip networks. Current capabilities are combinations of network security, cyber-resilient controllers, and anomaly detection that can raise the level of effort to penetrate and attack a SCADA system. The cyber security challenge for the instrumentation and controls network for an advanced small modular reactor extends beyond the usual best cyber practices. It requires implementation of strict configuration management and control practices of not only hardware and software components, but also planning and execution of proper concepts of operations (conops) that define physical and network access rights, software and hardware maintenance and upgrades—including supply chain management. Ongoing research to develop inherent resilience will result in mathematical techniques to successfully detect and continue system operation after a successful cyber penetration.

7.10 REFERENCES – CHAPTER 7

1. A. M. Melin et al., *A Mathematical Framework for the Analysis of Cyber-Resilient Control Systems*, ISRCS, 2013.
2. G. J. J. Ducard, *Fault-tolerant Flight Control and Guidance Systems*, Springer (2009).

8. ONGOING WORK

ORNL is leading the complementary dynamic simulations and controls project *Advanced SMR Dynamic System Modeling Tools* [1]. The toolset under development is envisioned to provide a guided-approach to allow users to develop power system models that are representative of SMR technology and end-to-end systems being proposed for deployment. The ability to design and model instrumentation and control equipment and strategies is an explicit part of the model capability.

The system package consists of a user interface to define reactor systems through component selection, arrangement, and parameter definition. The project selected Dymola/Modelica as the modeling platform.

The Modelica language has built-in features and open-source-toolsets for modeling fluid power systems. Physical systems are modeled by connecting *classes* of components in series or parallel, and by specifying the important parameters of the objects. Fluids are defined as special classes that model the medium behavior using *semi-empirical correlations* or *first-principle equation of state models* that yield the full state of the medium as a function of two known states (e.g., *pressure* and *enthalpy*). These models can be sophisticated enough to support a wide range of operating regimes for fluids at the cost of computation time—and sometimes numerical stability. These property functions are frequently called during execution of simulations to calculate various engineering variables such as heat transfer coefficients and friction factors. The properties of water are already built into the standard Modelica Fluid library. The built-in water class has a complex set of routines that support working with water from sub-cooled to supercritical regions. As part of the project, ORNL implemented a number of heat transfer media, including liquid salts (flibe, flinak, $KFZrF_4$), and liquid metals (sodium, NaK, PbBi eutectic) for use in Modelica.

8.1 ALMR PRISM END-TO-END SYSTEMS PACKAGE

The project selected General Electric's ALMR PRISM design developed for the U.S. Department of Energy under the *Advanced Liquid Metal Reactor* program as the reference advanced SMR plant going forward. This reactor class will be the first systems simulation package generated by this project. More reactor and plant systems classes will be added as the project continues.

Modelica offers a truly object-oriented programming experience. Once defined, objects can be instantiated and extended multiple times. This capability allows for quick manipulation of systems, subsystems and components.

As an example, an end-to end configuration of ALMR PRISM is shown in Fig. 55. This plant configuration includes only one intermediate heat exchanger (IHX) with 425 MW(t) thermal rating. The reactor core and primary heat transport system (PHTS), IHX primary (shell side) and intermediate (tube side) geometry, material parameters and fluid selections, intermediate heat transport system (IHTS), and power conversion system (PCS) parameters can be easily configured through the built-in user interface designed in Dymola. Alternatively, select model parameters can be configured by the Excel and web interfaces developed by the project team.

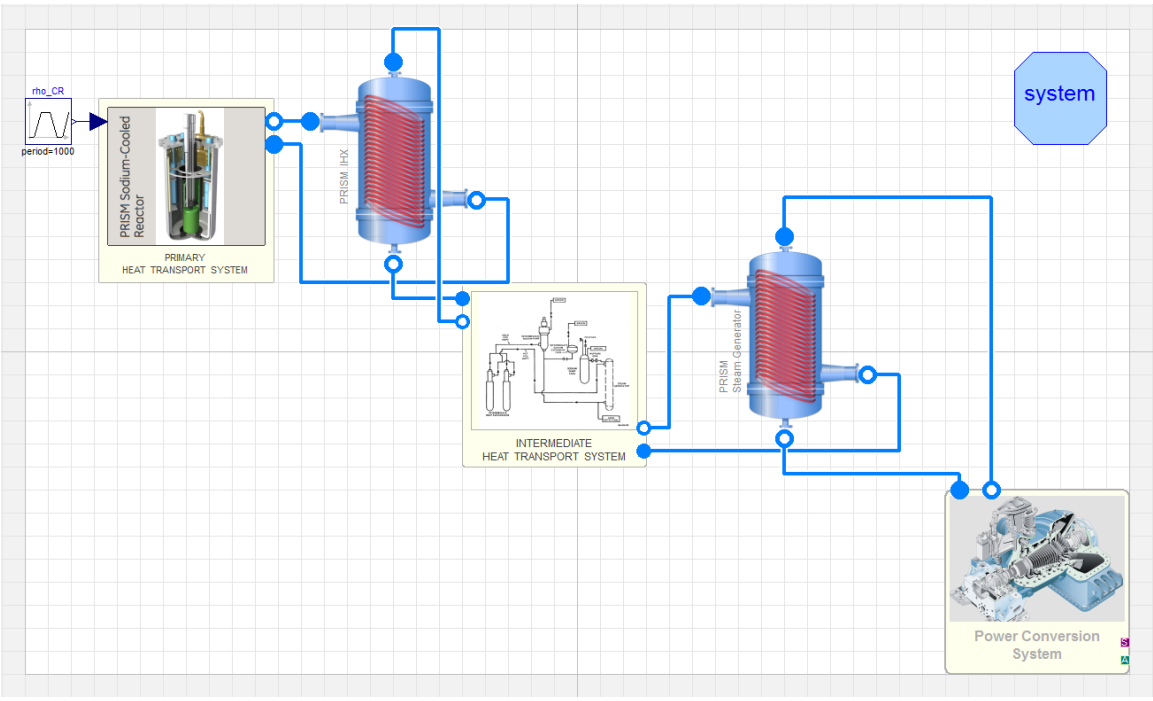


Fig. 55. Top-level block diagram for ALMR PRISM end-to-end plant with one IHX in Dymola/Modelica.

However, in the baseline ALMR PRISM design, each reactor module includes two IHXs connected to a single intermediate heat transport system. Each IHX has a thermal rating of 225 MW(t). As demonstrated in Fig. 56, the single IHX configuration can be easily reconfigured to include two IHXs as the baseline design uses. Going from one IHX configuration with 450 MW(t) thermal rating to two IHXs with 225 MW(t) thermal rating, each significantly changes the dynamic response. The latter configuration has much more fluid volume, which increases the thermal inertia contained in the IHTS.

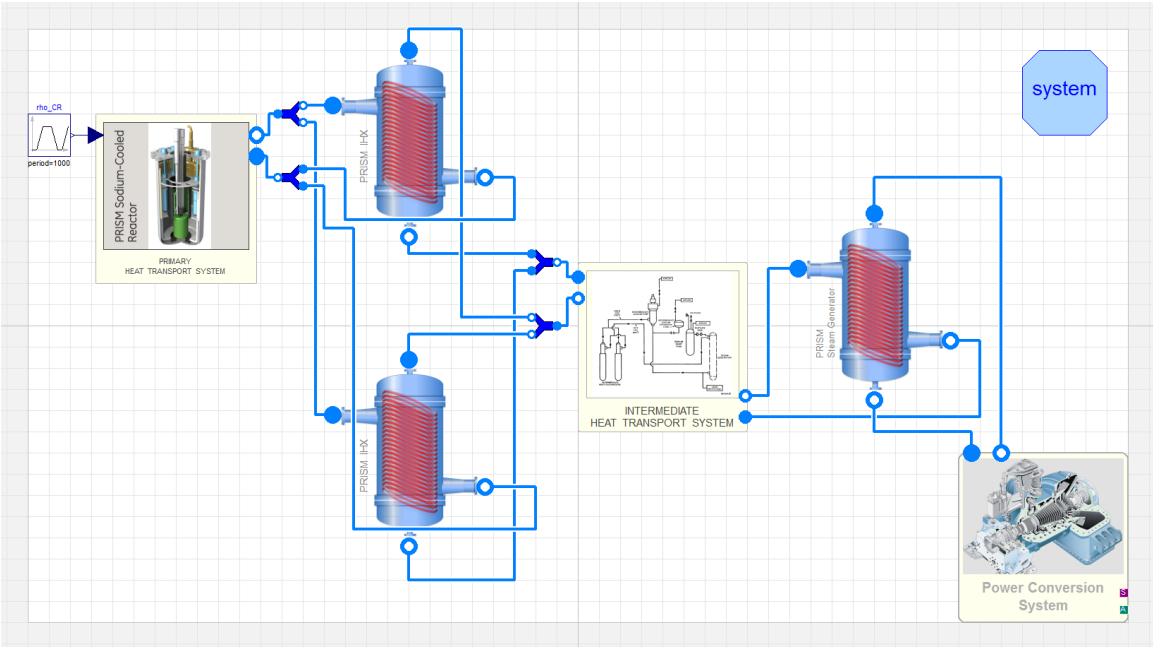


Fig. 56. Top-level block diagram for ALMR PRISM end-to-end plant systems with two IHXs.

For the supervisory control project, the toolset offers remarkable capabilities. Modelica is an open-source language developed specifically for multi-physics dynamic modeling. Furthermore, Modelica fully supports *hybrid simulations*.

Hybrid models contain two distinct behavior types: (1) continuous evolution, and (2) discrete-event evolution. Continuous evolution includes both continuous-time evolution and discrete-time evolution. However, discrete-time evolution and discrete-event evolution should not be confused. Discrete-time refers to a sampled representation of a continuous-time system, while discrete events are instantaneous transitions upon a certain trigger. An example would be opening or closing of a pump or trip of a turbine.

Traditionally, dynamic systems have been modeled in continuous-time modeling environments. However, in order to simulate the supervisory control system execution, the simulation environment must support both continuous-time evolutions and discrete-event evolutions, which is called a *hybrid* model.

8.1.1 Structures, Systems, Components, and Interfaces

As discussed earlier, the supervisory control system is being implemented in a hierarchical structure—with the continuous-time control at the lowest level and decision engine at the top level. In order to preserve this architecture, the simulation environment, and the developed system and component models must implement proper interfaces for exchange of information between the architectural layers. This should be done in a way that follows the interface and transparency rules as discussed in Section 4.5.

The supervisory control project team is working with the *Advanced SMR Dynamic Modeling Tools* project to help develop system and component definitions with proper interfaces, which are the communication channels that would transmit the supervisory controller commands to the *functional layer*, and similarly, receives sensor readings and fault indications for execute various decision-making strategies.

The reactor and the Primary Heat Transport System (PHTS) model, as shown in Fig. 57, can be used as an example. In this particular implementation, the primary loop contains only two major control variables: (1) reactor core temperature rise, and (2) primary coolant flow rate.

The data exchange is carried out using the *bus* object, which is implemented as an *expandable connector*. The control bus object is then connected to the *sensor* and *actuator* interfaces, which are then connected to the sensing or actuation objects. As explained earlier, systems in the path of the heat flow are Tier-I systems. All the sensing and actuation objects in the PHTS are Tier-I objects; hence they are controlled by the local feedback loop control system or an integrated control system (ICS).

Obviously, the reactor core and the PHTS do not offer much control options for the supervisory control system. The reactor core does contain emergency shutdown rods. However, these systems are controlled by the Reactor Protection System (RPS), therefore the supervisory control system is not permitted to interface with any safety or safety-related system—as per its functional requirements and the regulatory rules [1].

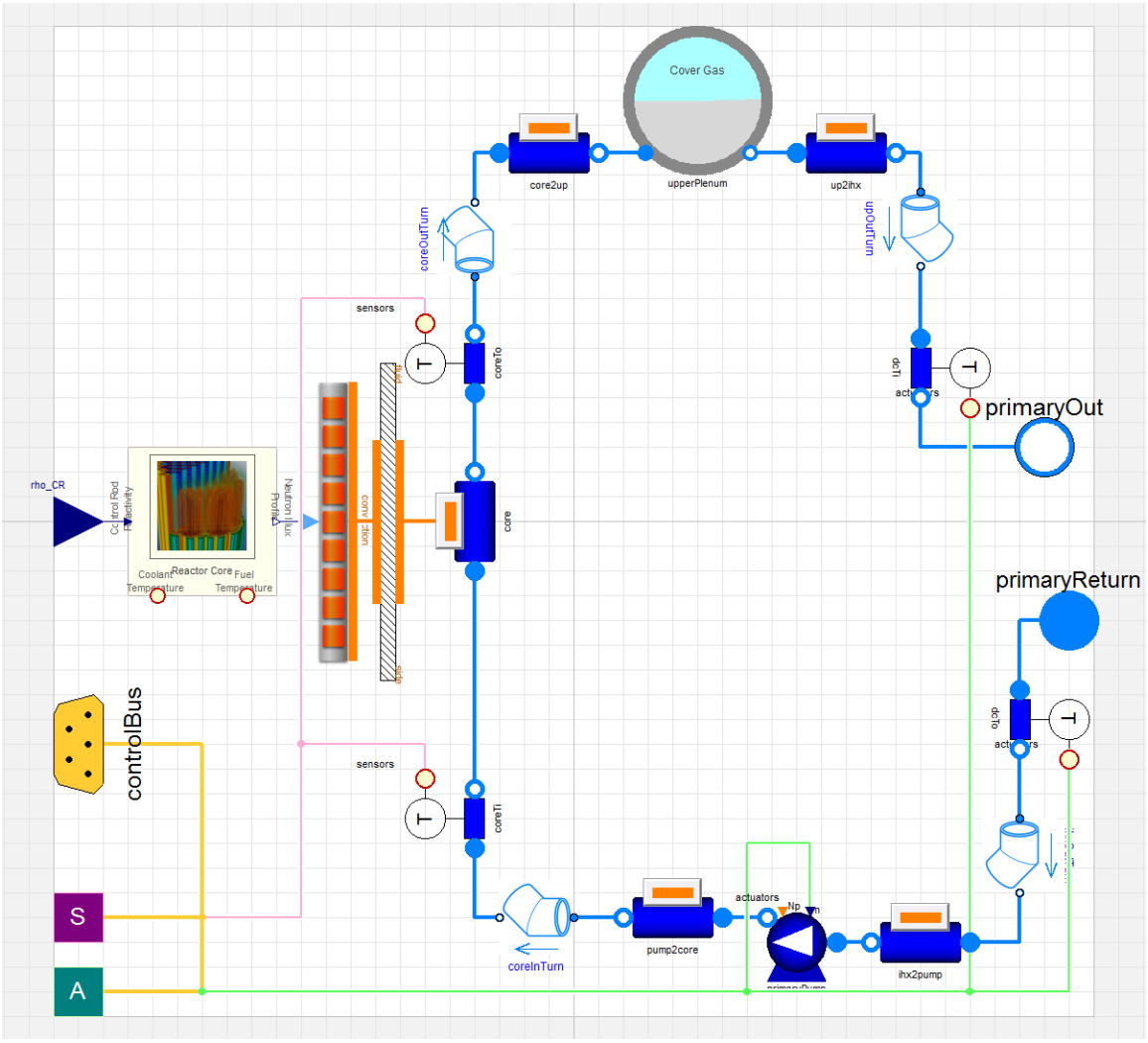


Fig. 57. ALMR PRISM reactor core and Primary Heat Transport System with sensing and actuation interfaces implemented in Dymola/Modelica.

While the PHTS only has Tier-I actuation interfaces, the PCS does contain a large number of Tier-II interfaces, as shown in Fig. 58, which represents the top-level diagram of the ALMR PRISM Power Conversion System (PCS). As can be seen in the figure, the system model has Tier-II interfaces that allow control of steam flow, such as `stopV1`, `stopV2` and `stopV3`, which are the *steam stop valves* from each of the three steam generators; `TCV`, which is the *turbine control valve* that allows regulation of turbine speed. The `bypassVALVE` object represents the *main steam bypass valve*, which is controlled by a logic code simulating the Reactor Protection System (RPS).[·]

At this point of the implementation, only certain high-level control instructions can be simulated. Once the *Decision-Making Module* and the *Command Generation Module* are implemented, it will allow simulation of representative instructions to the integrated control system or the Tier-II systems.

[·] The connection to the `bypassValve` actuator is for simulation purposes. In the actual configuration, the supervisory control system does not communicate with any safety or safety-related component.

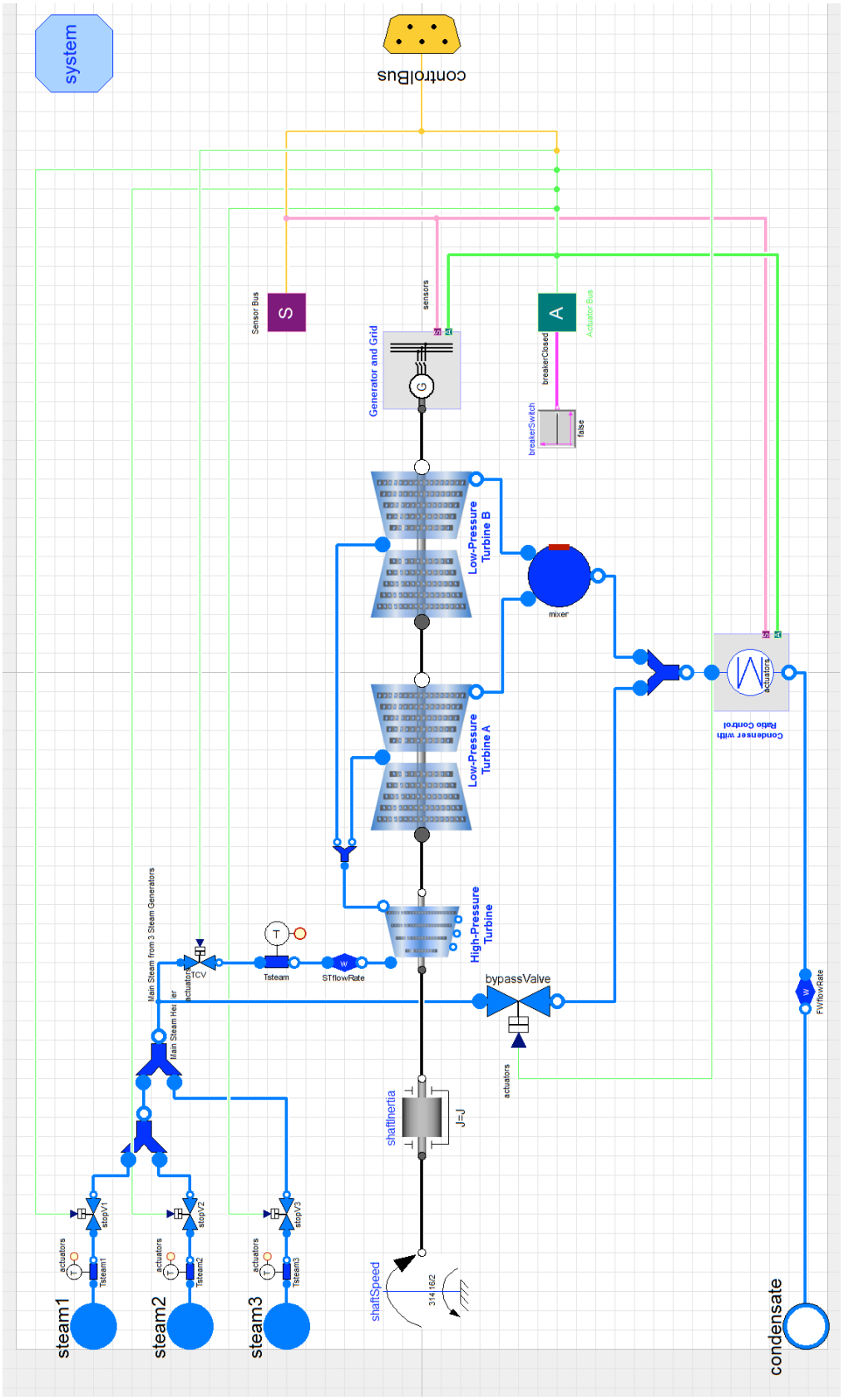


Fig. 58. A simplified version of sensing and actuation interfaces for the ALMR PRISM Power Conversion System implemented in Dymola/Modelica.

The Advanced SMR Dynamic Modeling Tools project is developing two control strategies for ALMR PRISM: (1) independent local feedback loop control with feedforward actions, and (2) an integrated control system using multivariate control. For the local loop strategy, the combination of feedforward and feedback actions is a key element in the control system design to overcome process delays while maintaining a smooth and stable response.

8.1.2 SysML to Modelica Translation

As briefly discussed in Section 2.3 of this report, the supervisory control project will use the SysML language to integrate the requirements-based engineering with the model-based engineering. The supervisory control functional requirements were developed during the first phase of the project, and the list was delivered in a report as part of Task 1 milestone [2].

Object Management Group (OMG) is an international computer industry standards consortium. OMG's modeling standards, including the *Systems Modeling Language* (SysML), *Unified Modeling Language* (UML) and *Model-Driven Architecture* (MDA), enable powerful development and execution of complex systems, such as modeling of end-to-end systems of a nuclear power plant.

OMG offers translation tools to convert SysML constructs to Modelica classes. Models implemented in SysML are automatically converted to model objects that can be executed from a development environment such as Dymola.

The advantage of this translation is that it automatically propagates the functional requirements as simulation constraints, which allows complete traceability, verification and validation of requirements.

SysML and UML languages are becoming more widespread in complex engineering applications. The project team considers that such implementation path will enable better industry acceptance of the concepts and methods developed for the supervisory control system.

8.2 REFERENCES – CHAPTER 8

1. L. Qualls, R. E. Hale, S. M. Cetiner, D. L. Fugate, *SMR Dynamic System Modeling Tool Update: April 2013*, ORNL/TM-2013/150, SMR/ORNL/IR-2013-01, Oak Ridge National Laboratory, Oak Ridge, TN (April 2013).
2. S. M. Cetiner, D. L. Fugate, R. A. Kisner, R. T. Wood, *Functional Requirements for Supervisory Control of Advanced Small Modular Reactors*, SMR/ICHMI/ORNL/TR-2013/03, Oak Ridge National Laboratory, Oak Ridge, TN (December 2012).

9. SUMMARY AND CONCLUSIONS

The potential benefits of an advanced SMR include more operational flexibility, reduced financial risk, high availability, and lower operating costs compared with traditional large-output nuclear power plants. In the tradition of larger plants, staffing of a multi-plant installation would require a full operations staff for each reactor. NRC regulations establish a minimum required staffing level per reactor control room. Future SMRs are likely to have one control room for multiple reactor modules. If the legacy minimum-staffing requirement is directly applied to SMRs, it will most likely result in prohibitive staffing costs (operational and maintenance). The current industry average for plant staffing to conduct operations and maintenance activities is roughly about one person for every 2 megawatts. Thus, a typical 1000 MW(e) large plant will staff approximately 500 personnel. The desired target objective would be to staff future SMRs with a minimum staffing level based on the control room rather than the number of reactor units. Increased capabilities in automation, human machine interfaces, decision-making, and control can enable this staffing efficiency with desired control system performance in normal and off-normal conditions.

This research uses the ALMR PRISM as the baseline advanced SMR design both for the current study and for future modeling and simulation. The ALMR PRISM small modular reactor design had previously undergone a level of design that makes it a good reference, and much of the information is publically available. The reference plant and its control system are described in the report. The ALMR PRISM control architecture concepts are complementary and similar to the concepts developed through this project. In fact, after examining supervisory control in several applications domains, the study concludes supervisory architectures, although containing unique features to each application, share many common features and structures.

The present research defines a structure and architecture of a supervisory control system for advanced SMRs that has the features of planning and scheduling, analyzing plant status, diagnosing problems as they develop and predicting potential future problems, making decisions based on these features, and generating validated commands to lower structures in the plant. For control purposes, the plant is divided into three tiers, corresponding to a system's relationship to the main flow of energy through the plant—that is, from the reactor to the generator and the ultimate heat sink (UHS).

Tier-I systems involve the direct pathway of transporting heat from the source to the sink. Tier-II systems provide direct support to Tier-I systems. Tier-III systems are the common utilities and services that supply bulk materials to the Tier-I and Tier-II systems. The supervisory control concepts and architectures developed in this research apply to the Tier-I and Tier-II systems.

The functions of the supervisory control system are designed to require minimal human intervention in both normal and abnormal operations. One of the chief functions of the supervisory control systems is to prevent excursion into the trip regime of the reactor protection system. This function is accomplished by vigilant monitoring of equipment status, measured parameters, predicted outcomes, and internal states to make decisions that generate appropriate set points, valve alignments, and other configuration structures.

Concepts of metrics of effectiveness for supervisory control were investigated. Because information is the principal part of the decision-making process, information entropy can be used as a measure of the uncertainty in that information and hence the decision-making process. Information entropy was investigated as a method to compare control architectures. An automatic depressurization system was used a test example to compare a probabilistic risk-based assessment against an entropy-based assessment. The entropy-based method correlated well in the limited test. The entropy-based method has application in evaluating disparate architectures. In addition, this method has potential for on-line, real-time estimation of system uncertainty in the decision-making process.

The cyber infrastructure for a SMR requires a combination of defenses that protects both I&C networks and information (e.g., plant or corporate) networks. Current capabilities are combinations of network security, cyber-resilient controllers, and anomaly detection that can raise the level of effort needed to penetrate and attack a supervisory control and data acquisition (SCADA) system. The cyber security challenge for the instrumentation and controls network for an advanced SMR extends beyond the usual best cyber security practices. It requires implementation of strict configuration management and control practices of not only hardware and software components but also planning and execution of proper concepts of operations (CONOPS) that define physical and network access rights and software and hardware maintenance and upgrades—including supply chain management. Ongoing research to develop inherent resilience in real-time feedback controllers will result in mathematical techniques to successfully detect and continue system operation after a successful cyber penetration.

APPENDIX A

COMPLETE LIST OF SYSTEMS IN ALMR PRISM

APPENDIX A.

COMPLETE LIST OF SYSTEMS IN ALMR PRISM

This list of ALMR PRISM plant systems, as presented in Table A.1, was derived from the PRISM Preliminary Safety Information Document [1].

Table A.1. Complete list of systems in ALMR PRISM and their shared status

Systems in ALMR PRISM

(A *plant* consists of three *power blocks*, with three *reactor modules* (NSSS Systems)/power block.)

System Name	Common System Between Modules	Plant-Wide Shared System
Primary Heat Transport System	—	—
Intermediate Heat Transport System	—	—
Sodium-Water Reaction Pressure Relief Subsystem (IHTS)	—	—
Steam Generator and Water/Steam Subsystem (Steam Generator System)	X	—
Leak Detection Subsystem (Steam Generator System)	X	—
Water Dump Subsystem (Steam Generator System)	X	—
Auxiliary Cooling Subsystem (Steam Generator System)	X	—
Reactor Vessel Auxiliary Cooling System (Shutdown Heat Removal Systems)	—	—
Auxiliary Cooling System (Shutdown Heat Removal Systems)	—	—
Containment Systems	—	—
Plant Control System (PCS)	X	X
Power Block Control System	X	—
Module Control System	—	—
Local Control System	—	—
Reactor Protection System (RPS)	—	—
Radiation Monitoring System (I&C)	X	X
Fire Protection Monitoring (I&C)	X	X
Impurity Monitoring System	X	X
Refueling Neutron Flux Monitor (I&C)	—	—
Diagnostic Monitoring (I&C)	—	—
Loose Parts Monitoring (LPM) (I&C)	—	—
Data Handling and Transmission System (DHTS)	X	X
Plant Control Complex (includes MMI)	X	X
Preferred Offsite Power System (unit aux power system)	X	X
Secondary Offsite Power System (common station service system)	X	X
Onsite AC Power System	X	X

Table A.1. (continued)

Systems in ALMR PRISM

(A *plant* consists of three *power blocks*, with three *reactor modules* (NSSS Systems)/power block.)

System Name	Common System Between Modules	Plant-Wide Shared System
Essential 120 V ac power	X	—
Onsite DC Power System	X	—
Uninterruptable Power Supply (UPS) systems	X	—
Electromagnetic Pumps Power Supply	—	—
Reactor Fuel Handling System (Reactor Refueling System)	X	—
In-Vessel Transfer Machine (IVTM) (Reactor Fuel Handling System)	—	—
Fuel Receiving, Storage and Shipping System (Reactor Refueling System)	—	X
Refueling Enclosure (Transport System) (Reactor Refueling System)	—	X
Fuel Transfer Cask (Transport System) (Reactor Refueling System)	—	X
Cask Transporter (Transport System) (Reactor Refueling System)	—	X
Overall Refueling Control System	—	X
Plant Service Water System	—	X
Turbine Plant Component Cooling Water System	X	—
Chilled Water System	—	X
Makeup Water Treatment Subsystem (Treated Water System)	—	X
Steam Generator Blowdown Cleanup Subsystem (Treated Water System)	—	X
Potable Water Subsystem (Treated Water System)	—	X
Chemical Feed Subsystem (Treated Water System)	—	X
Water Source System (water to cooling tower basins; raw water supply)	—	X
Waste Water Disposal Subsystem (Wastewater Treatment System)	—	X
Sanitary Waste Disposal Subsystem (Wastewater Treatment System)	—	X
Inert Gas Receiving and Processing System (IGRPS) (He, Ar, N Subsystems)	—	X
Impurity Monitoring and Analysis System	X	X
Compressed Air Systems (service air, instrument air)	—	X
Plant Heating, Ventilation, Air Conditioning Systems (HVAC)	—	X
Sodium Receiving and Transfer Subsystem (Auxiliary Liquid Metal System)	—	X
Intermediate Sodium Processing Subsystem (ISPS) (Auxiliary Liquid Metal System) (also called Purification System)	—	X
Primary Sodium Processing Subsystem (PSPS) (Auxiliary Liquid Metal System) (also called Purification System)	—	—
Piping and Equipment Heating and Insulation System	—	X

Table A.1. (continued)

Systems in ALMR PRISM

(A *plant* consists of three *power blocks*, with three *reactor modules* (NSSS Systems)/power block.)

System Name	Common System Between Modules	Plant-Wide Shared System
Plant Fire Protection System (Na and non-Na fire protection)	—	X
Communication System	—	X
Turbine-Generator	X	—
Main Steam System	X	—
Main Dump System	X	—
Extraction Steam System	X	—
Auxiliary Steam System	—	X
Main Condenser Subsystem (Heat Rejection System)	X	—
Condenser Air Extraction Subsystem (Heat Rejection System)	X	—
Circulating Water Subsystem (Heat Rejection System)	X	—
Feedwater System	X	—
Condensate System	X	—
Feedwater Heater Drain System	X	—
Auxiliary Boiler Feedwater and Condensate System	—	X
Intermediate/low Activity Level Liquid System (Liquid Waste Management Systems)	—	X
Detergent and Decontamination Liquid System (Liquid Waste Management Systems)	—	X
Gaseous Waste Management Systems	—	X
Portable Helium Gas Supply System (including storage/transfer tank)	—	X
Solid Waste Management System	—	X

Each of the system response event trees for the initiating events for ALMR PRISM contains the following systems.

- *Reactor Protection System (RPS)*: This system senses the need to shut down and initiates the proper signals for power, flow, and heat removal control.
- *Reactor Shutdown System (RSS)*: This system includes the control rods, control rod drive motors, and magnetic latches.
- *Inherent Reactivity Feedback Features*: These features include the control rods, their drivelines and their guide tubes, the core restraint system, load pads of the core assemblies, and the grid plate.
- *Primary Pumps*: This includes the primary pumps and their power supply.
- *Pump Coastdown System*

- *Operating Power Heat Removal System* (via balance of plant)

- Shutdown Heat Removal via IHX or RVACS

The plant shall be designed to maximize sharing of services and facilities. The standard design shall employ common facilities and three power blocks with each power block consisting of three Nuclear Steam Supply Systems (NSSS) and one turbine-generator. Design of the NSSS shall permit other power block design arrangements to be feasible, including two or four NSSS's per turbine. The NSSS, its associated systems, and plant layout shall be designed to permit incremental additions or removals of power-generating capability with minimal interruptions to other operating NSSS's.

REFERENCES – APPENDIX A

1. General Electric, *PRISM Preliminary Safety Information Document*, prepared for the US Department of Energy Under Contract No. DE-AC03-85NE37937, December 1987.