

Enabling Autonomous Control For Space Reactor Power Systems

Richard T. Wood

Oak Ridge National Laboratory; P.O. Box 2008, Oak Ridge, TN, 37831

E-mail: WoodRT@ornl.gov

Abstract—The application of nuclear reactors for space power and/or propulsion presents some unique challenges regarding the operations and control of the power system. Terrestrial nuclear reactors employ varying degrees of human control and decision-making for operations and benefit from periodic human interaction for maintenance. In contrast, the control system of a space reactor power system (SRPS) employed for deep space missions must be able to accommodate unattended operations due to communications delays and periods of planetary occlusion while adapting to evolving or degraded conditions with no opportunity for repair or refurbishment. Thus, a SRPS control system must provide for operational autonomy.

Oak Ridge National Laboratory (ORNL) has conducted an investigation of the state of the technology for autonomous control to determine the experience base in the nuclear power application domain, both for space and terrestrial use. It was found that control systems with varying levels of autonomy have been employed in robotic, transportation, spacecraft, and manufacturing applications. However, autonomous control has not been implemented for an operating terrestrial nuclear power plant nor has there been any experience beyond automating simple control loops for space reactors. Current automated control technologies for nuclear power plants are reasonably mature, and basic control for a SRPS is clearly feasible under optimum circumstances. However, autonomous control is primarily intended to account for the nonoptimum circumstances when degradation, failure, and other off-normal events challenge the performance of the reactor and near-term human intervention is not possible. Thus, the development and demonstration of autonomous control capabilities for the specific domain of space nuclear power operations is needed.

This paper will discuss the findings of the ORNL study and provide a description of the concept of autonomy, its key characteristics, and a prospective functional architecture that can support SRPS control for an extended deep space mission. The desirable characteristics of autonomous control include intelligence, robustness, optimization, flexibility, and adaptability. The degree of autonomy that is necessary for a given mission will depend on resource constraints, performance goals, operational complexity, technological capabilities, and mission risk considerations. The prospective architectural framework employs a hierarchical structure to integrate needed control, diagnostic, and decision functions and thus enable autonomy.

I. INTRODUCTION

Under Project Prometheus, the National Aeronautics and Space Administration (NASA) has been considering deep space missions that would utilize a space reactor power system (SRPS) to provide energy for propulsion and spacecraft power. A SRPS provides the opportunity to supply high-sustained power for space applications that is both reliable and mass efficient.

Terrestrial nuclear reactors employ varying degrees of human control and decision-making for operations and benefit from periodic human interaction for maintenance. In contrast, the control system of a SRPS utilized for a deep space mission must be able to provide continuous operation for the mission duration with limited immediate human interaction and no opportunity for hardware maintenance or sensor calibration. In effect, the SRPS control system must be able to independently operate the power plant while maintaining power production even

when subject to off-normal events and component failure. This capability is critical because it will not be possible to rely upon continuous, immediate human interaction for the control of the power plant due to communications delays and periods of planetary occlusion. In addition, uncertainties, rare events, and component degradation combine with the aforementioned inaccessibility and unattended operation to pose unique challenges that a SRPS control system must accommodate. Autonomous control is needed to address these challenges and optimize the reactor control design.

II. STATE OF THE TECHNOLOGY

To support Project Prometheus, Oak Ridge National Laboratory (ORNL) conducted an investigation of autonomous control. Overviews of autonomous control characteristics, capabilities, and applications were found that establish the existing experience and current technology readiness.^{1,2,3,4,5,6}

Control systems with varying levels of autonomy have been employed in robotic, transportation, spacecraft, and manufacturing applications. However, autonomous control has not been implemented for an operating terrestrial nuclear power plant, and there has not been any experience beyond automating simple control loops for space reactors. Current automated control technologies for nuclear power plants are reasonably mature, and basic control for a SRPS is clearly feasible under optimum circumstances. However, autonomous control is primarily intended to account for the non-optimum circumstances when degradation, failure, and other off-normal events challenge the performance of the reactor, and near-term human intervention is not possible. There are clear gaps in the development and demonstration of autonomous control capabilities for the specific domain of nuclear power operations.

II.A. Advanced Control in Nuclear Power Applications

In the nuclear power industry, single-input, single-output classical control has been the primary means of automating individual control loops. The use of multivariate control, such as three element controllers for steam generators, has been employed in some cases. In a few cases, efforts were made to coordinate the action of individual control loops based on an overall control goal and extend the range of automated control.

The application of most advanced techniques for nuclear power control has primarily been the domain of universities and national laboratories [e.g., the U.S. Department of Energy (DOE) Advanced Controls Program at ORNL in the late 1980s and early 1990s]. Some of the techniques employed in controls research for both power and research reactors include adaptive robust control for the Experimental Breeder Reactor II (EBR-II), fuzzy logic control for power transition, H-infinity control and genetic algorithm-based control for steam generators, neural network control for power distribution in a reactor core, and supervisory control for multimodular advanced liquid-metal reactor (ALMR). Proceedings of Past Topical Meetings on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies provide a useful compendium of findings from such research activities.^{7,8,9,10}

II.B. Autonomy in Space Exploration

NASA has pursued autonomy for spacecraft and surface exploration vehicles (e.g., rovers) to reduce mission costs, increase efficiency for communications between ground control and the vehicle, and enable independent operation of the vehicle during times of communications blackout. For rovers, functional autonomy addresses navigation, target identification, and

science package manipulation. For spacecraft, functional autonomy has focused on automated guidance, navigation, and control.

Autonomy for rovers has progressed during the last decade with prominent examples from efforts to explore the surface of Mars. The Mars Pathfinder rover, Sojourner, explored the Martian terrain beginning in July 1997.¹¹ The Sojourner had very limited autonomy to enable navigation and provide for resource management and contingency response. Because it only provided supervised autonomy, repetitive ground monitoring was required. In January 2004, Spirit and Opportunity, the twin Mars Exploration Rovers (MERs), began a surface exploration mission that has continued into 2006. These rovers employ expanded autonomy over what was feasible for Sojourner and provide model-based recovery, resource management, and autonomous planning capabilities in addition to autonomous obstacle detection and navigation. The integration software architecture used to facilitate MER autonomy is the “Coupled Layer Architecture for Robotic Autonomy” (CLARATy).¹² CLARATy provides a dual-layer architecture consisting of a decision layer for artificial intelligence (AI) software and a functional layer for controls implementations. Implicit granularity in each layer allows for a functional hierarchy with nested capabilities.

Spacecraft autonomy has been demonstrated with the Deep Space 1 mission. Deep Space 1 was launched in October 1998 as a test platform to validate high-risk advanced technologies in space.¹³ In addition to demonstrating autonomous navigation of the spacecraft, a principal experiment involved demonstration of an AI system for on-board planning and execution of spacecraft activities. During the Deep Space 1 mission, the remote agent (RA) AI system was activated to control the spacecraft for a limited period. Testing of the RA capabilities involved an experiment that included the injection of four simulated faults. A software flaw in the executive module of the RA was detected and diagnosed, so a second experiment was conducted to fulfill the remaining objectives of the test.

III. AUTONOMOUS CONTROL FUNCTIONAL DEFINITION

III.A. The Nature of Autonomy

There is a distinction between automated control and autonomous control. Consideration of the Greek root words illustrates the difference. *Automatos* means self-acting, while *autonomos* means independent. Similarly, automated control involves self-action, while autonomous control involves independent action. Autonomous control implies an embedded intelligence. Although automation

includes at least a limited inherent authority within the control system, automated control often consists of straightforward automatic execution of repetitive basic actions. It is clear that autonomous control encompasses automated control.

Automated control provides control actions that result from fixed set of algorithms with typically limited global state determination. As a result, automated control is often implemented as rigidly defined individual control loops rather than as fully integrated process/plant control. Although automated control requires no real-time operator action for normal operational events, most significant decision-making is left to the human rather than incorporated as part of the control system. In contrast, autonomous control integrates control, diagnostic, and decision capabilities. A flexible functional architecture provides the capability to adapt to evolving conditions and operational constraints and even support self-maintenance over the control system lifetime. While automated control is common in numerous applications, autonomous control is more difficult to achieve, and the experience base is very limited.

Autonomy extends the scope of primary control functions. Such capabilities can consist of automated control during all operating modes, process performance optimization (e.g., self-tuning), continuous monitoring, and diagnosis of performance indicators as well as trends for operational and safety-related parameters, diagnosis of component health, flexible control to address both anticipated and unanticipated events and to provide protection of life-limited components (such as batteries and actuators), adaptation to changing or degrading conditions, and validation and maintenance of control system performance.

Key characteristics of autonomy include intelligence, robustness, optimization, flexibility, and adaptability. Intelligence facilitates minimal or no reliance on human intervention and can accommodate an integrated, whole system approach to control. It implies embedded decision-making and management/planning authority. Intelligence in control provides for anticipatory action based on system knowledge and event prediction. To support control and decision, real-time diagnostic/prognostic capabilities are important for state identification and health/condition monitoring. Additionally, self-validation is an aspect of intelligence that addresses data, command, and system performance assessment and response.

In addition to providing an environmentally rugged implementation, robustness is addressed by accounting for design uncertainties and unmodeled dynamics. Fault management is an important consideration in achieving

robustness. Fault management involves fault avoidance, fault removal, fault tolerance, and fault forecasting. Fault avoidance can be accomplished through approaches such as the use of formal methods for software design, the application of an object-oriented paradigm for the software architecture, and software module reuse. Fault removal can be promoted through formal inspections of software, data flow testing, and fault injection testing (e.g., either state-based or code-based). Fault tolerance can involve redundancy, design diversity, high-reliability implementation, or error detection and recovery functionality. Fault forecasting techniques include reliability modeling, data collection and data-driven modeling, operational profiling, and rare event prediction. Finally, robustness can also involve self-maintenance or self-healing. This capability is promoted through means such as captured design knowledge and self-correcting features, prognostics to identify incipient failure, and fault detection and isolation.

Optimization implies rapid response to demands, minimal deviation from target conditions, and efficient actuator actions. Optimized control can be facilitated by self-tuning and other forms of adaptation. Flexibility and adaptability are enabled by diverse measurements, multiple communication options, and alternate control solutions. Functional reconfigurability facilitates the effective use of these systems options, while an inherent redesign capability permits adaptation to unanticipated conditions.

The characteristics discussed above represent the possibilities of autonomy, but they do not constitute a necessary set. Therefore, autonomous control can be viewed as providing a spectrum of capabilities with automated control representing the lowest extreme or baseline of the continuum. The incorporation of increasing intelligence and fault tolerance moves the control capabilities further along the spectrum. The higher degrees of autonomy are characterized by greater fault management, more embedded planning and goal setting, and even self-healing. The realization of full autonomy involves learning, evolving, and strategizing independent of human interaction or supervision.

III.B.Space Nuclear Powers Mission Challenges

The space reactor control and protection paradigm is different from conventional terrestrial reactor applications. Terrestrial reactors have relied upon immediate interaction from readily available human resources. This includes varying degrees of direct human control and decision making for operations and periodic human intervention for maintenance and refurbishment. In contrast, the SRPS control system must be able to provide continuous, remote, often-unattended operation

for a mission lasting up to a decade or more. Because of communication delays and blackouts, immediate human interaction for continuous operational supervision and event management is not feasible. This isolation drives the need for a high level of autonomy. Because of launch considerations, size and mass constraints significantly limit the options for redundancy and diverse systems. This limitation drives the need for functional and environmental robustness. Because of distance from Earth for deep space or planetary surface power applications, maintenance and refurbishment are improbable if not impossible. This inaccessibility drives the need for long-life dependability. Finally, because of the critical and time-sensitive nature of some spacecraft maneuvers, space reactor power must be available on demand. This operational imperative, coupled with the likelihood that a SRPS restart capability will be unavailable, requires that reactor scrams as a response to plant events must be minimized if not completely avoided. Thus, unlike terrestrial nuclear power plants, mission assurance must be emphasized over reactor protection.

Automated control can provide the necessary automation of normal operational control to permit ground control personnel to assume a supervisory role for a SRPS rather than taking on direct, active control responsibilities. This control capability for full-power range maneuverability, including startup, has been previously developed and demonstrated for terrestrial reactors.¹⁴ However, considering the challenges of a deep space mission, the SRPS control system must do more than provide automated control of normal operational activities. In addition to automation, the control system must provide a level of autonomy that can detect, diagnose, and adapt to evolving conditions (e.g., failures or degradation) as well as rapidly respond to anticipated events without requiring a reactor scram. As a result, autonomous control is clearly necessary to ensure the successful application of a SRPS for deep space missions. This conclusion is based on the understanding that autonomous capabilities permit the SRPS control system to satisfy essential control objectives under significant uncertainties, disturbances, and degradation without requiring any human intervention. In a sense, the role of the autonomous control system is to act as an extension of and occasional proxy for the ground-based human operators to assure reliable, continuous operation of the SRPS over an extended lifetime under adverse conditions.

III.C. Space Nuclear Power System Control

Autonomous control functions of the SRPS can be defined based on the expected operational modes, which include startup, normal power operation, reactor protection, contingent operation, and end-of-mission

shutdown. As a minimum requirement of autonomy, the SRPS control system must be able to switch between normal operational modes automatically (i.e., automatic control). Additionally, reactor protective action must be available if the desired operational conditions cannot be achieved.

The phases of power operation include power ascension, steady state power and load following, and power reduction. Under normal conditions, power operation can be relatively simple, with inherent feedback effects serving to maintain stability and provide the means for load following in response to minor fluctuations. Thermal load transients (e.g., turbine failure) can be treated as off-normal events. Other off-normal events include design uncertainties, load/power interruptions, control element jamming, control motor burn out, control linkage failure, control element unintended motion, actuator signal interruption or interference, heat rejection system degradation or damage, control processor fault, rare-event software error, sensor failure, sensor signal interruption or interference, sensor drift, signal conditioning electronics drift, sensor noise increase, and communication failures or retransmissions. The most likely protective action would consist of a rapid power runback. Contingent operation occurs when SRPS operation may be restricted either because of environmental limitations, such as an abnormal thermal environment, or because of power system limitations, such as component failures.

The response to off-normal events is where autonomy becomes especially relevant. The autonomous response includes a reflexive element and a deliberative element. The first element addresses reactor protection. Unlike terrestrial reactors, in which the primary defense against potentially adverse conditions resulting from off-normal events is to scram the reactor, it is quite likely that the SRPS must not shut down until the end of the mission because a restart capability may not be feasible. Thus, reactor protection is provided through diversity and defense-in-depth to anticipate potential challenges to power operation. A limitation system is one means of protecting the reactor. This is accomplished by defining acceptable operational regimes and over-riding control actions that would drive the reactor conditions to violate the limitation boundaries. In effect, the limitation system acts as a bounding system whose primary purpose is to provide a check against operations outside of analyzed conditions. The principle response of the limitation system would be to run back the reactor power to assume a safe low-power condition when necessary. Because of the operational imperative that power must remain available during critical spacecraft actions for deep space missions, the SRPS control system must provide the capability to switch out the protection element (or at least

expand the operational boundaries it maintains) on demand from the spacecraft or mission control.

The second element of the response to off-normal events addresses mission assurance. The deliberative nature (i.e., determination and decision) of this element contributes the most relevant attribute of autonomous control that distinguishes it from conventional automation. In the operational control context, the autonomous control functionality involves detection and immediate response to degraded or failure conditions. Fault management is a crucial part of this element of autonomous control, which provides for detection, diagnosis, and adaptation (or reconfiguration) given changing SRPS conditions. An additional aspect of this deliberative element is the monitoring, diagnosis, and validation of control system and SRPS performance. Through this capability, the SRPS control system is able to identify incipient events (transients or failures) for anticipatory rather than reactionary action, determine measures to protect life-limited or vulnerable components, and ensure continued dependable operation of the power plant.

As noted, the SRPS autonomous control functionality revolves around automated control for normal operational modes. In essence, the primary function of the control system is command generation to achieve the desired operational state. Additional functionality to support confirmation of control system performance includes features such as command verification, control coordination with interconnected systems, and strategy enforcement. Mechanisms for implementing these features can involve multiple diverse algorithms for comparison with the principal controller command, inclusion of feedforward action or some representation of unmodeled dynamics (e.g., exogenous variables) in control algorithms, event management according to predetermined sequences of events, and adaptation of the control strategy.

Performance management as part of the SRPS autonomous control functionality involves continuously assessing the condition of the control system and the SRPS to identify when predetermined adjustments to the controller should be invoked. The needed assessments include monitoring control system effectiveness, identifying the dynamic state of the SRPS, and determining the condition of key components. Methods that can be employed are state estimation algorithms, process system diagnostics, component condition monitoring, and control parameter adaptation.

Data management and communications are related capabilities with traditional and autonomous functionality intended to support autonomy and system integration.

Data acquisition and signal processing methods provide the data needed for control and monitoring, while signal validation adds information about data quality. For communications, the functional elements include device-level data and control signals, system-level information and commands, and spacecraft-level status and demands. The effective integration of data and information at each level requires a well-defined functional architecture with a capable physical infrastructure that supports reliable, timely information flow.

Desired functionality for fault management includes detection and identification of field device faults, change tracking for system parameters, detection of off-normal transients and identification of anticipated events, and configuration control. Field device monitoring can be accomplished through model-based and/or data-driven algorithms. Parameter tracking can involve empirical models or first principles estimation. Each capability can be used to facilitate an adjustable system dynamic model that can be used for fault prediction or control system performance validation. Finally, configuration control functions are needed to manage transitions among predefined control strategies or algorithms for the autonomous control system. This is essential for effective fault recovery.

To illustrate the autonomous functionality that can be provided for the SRPS control system, two fault management scenarios are considered in which detection and response are described. The first scenario relates to fault adaptation in the case of sensor failure. The indicators from surveillance and diagnostic functions that the SRPS control system can employ include divergence of redundant measurements, conflict between predicted (based on analytical or relational estimation) and measured values, and detection and isolation of a confirmed fault using an FDI algorithm. The prospective response can include substitution of a redundant measurement or utilization of a diverse measurement. An example of the latter would be using neutron flux instead of temperature (i.e., core thermal power) as a power measurement. Switching to an alternate control algorithm may prove necessary for faulted or suspect measurements.

The second scenario relates to fault avoidance in the case of a degrading actuator. The indicators of an incipient failure can be prediction of actuator failure based on prognostic modeling (e.g., fault forecasting) or detection of sluggish response to commands. The prospective response can be to switch to an alternate control strategy to avoid incipient failure by reducing stress on the suspect component. An example would be utilizing manipulation of core heat removal (e.g., coolant density change) instead of direct reactivity insertion (e.g., control element movement) to control reactor power.

III.D. Enabling Autonomous Control

Autonomous control must be addressed early in the design of the SRPS to determine the degree of autonomy required. Mission requirements, technology readiness, design trade-offs, and resource constraints will affect the autonomous capabilities to be included. The extent to which the key characteristics of autonomy are realized depends on the level of responsibility that is to be entrusted to the autonomous control system and the degree of mission risk the autonomous control system must mitigate.

Several factors can influence the degree of autonomy selected for a SRPS control system. These factors include the potential for human interaction (which is physically limited but also may be practically limited due to the economics of maintaining a ground-based team), performance goals, complexity of system demands, technological constraints, mission risk considerations, and the balance between simplicity (i.e., reliability) and complexity (i.e., the capacity to detect and adapt). The trade between reliability and mission assurance profoundly affects the level of autonomy employed for SRPS control. While having a highly reliable SRPS control system is important, that fact is meaningless if it cannot accommodate SRPS degradation. In such a case, the result is a highly reliable control system that becomes useless because the plant has changed.

Finally, as previously described, the experience base for autonomous control is not deep. In particular, autonomous control has not been implemented for an operating terrestrial nuclear power plant. The technology gaps indicated by investigation of the state of the technology for reactor control in general and autonomous control in particular indicate research, development, and demonstration (RD&D) activities that need to be accomplished to fully realize the goal of autonomous control for a SRPS. Key elements of the needed RD&D effort involve establishing a suitable functional architecture, developing foundational modules to support autonomy, and demonstrating the integrated application of autonomous capabilities.

IV. FUNCTIONAL ARCHITECTURE FOR AUTONOMOUS CONTROL

IV.A. Architectural Approaches

As observed from examples of autonomous control for nuclear and space applications, the principal functional architectures that have been employed, in most cases, involve some form of hierarchical framework with varying distributions of intelligence.

A three-level hierarchy is typical for robotic applications.^{1,15,16} The general concept of the hierarchy is that commands are issued by higher levels to lower levels and response data flows from lower levels to higher levels in the multitiered framework. Intelligence increases with increasing level within the hierarchy. Each of the three interacting tiers has a principle role. Basically the functional layer provides direct control, the executive layer provides sequencing of action, and the planner layer provides deliberative planning.

As previously described, an autonomous control architecture, based on the CLARAty software environment, was developed to support the MER mission. The CLARAty dual-layer architecture provides an upper (decision) layer for AI software and a lower (functional) layer for controls implementations. The development of CLARAty addresses perceived issues with the three-tiered architecture.¹² 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, trees 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.

The functional layer is an object-oriented hierarchy that provides access to the capabilities of the plant/system hardware and serves as the interface for the decision layer to the subject (robot, spacecraft, plant) under control. The interaction between the two layers depends on the relative granularity of each layer at the interface. At lower granularity, the decision layer has almost direct access to the basic capabilities of the plant/system. At higher granularity, the decision layer provides high level commands that are broken down and executed by the intelligent control capability of the functional layer. The decision layer provides functionality to break down goals into objectives, establish a sequential task ordering based on the plant/system state and known constraints, and assess the capability of the functional layer to implement those commands. At lower granularity within the decision layer, executive functions such as procedure enforcement are dominant while, at higher granularity,

planning functions such as goal determination and strategy development are dominant.

There is an architectural approach for nearly autonomous control systems that has been applied through simulated nuclear power applications (see Figure 1). As part of research into advanced multimodular nuclear reactor concepts, such as the International Reactor Innovative and Secure (IRIS) and the ALMR, a supervisory control system architecture was devised.¹⁷ This approach provides a framework for autonomous control while supporting a high-level interface with operations staff, which 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 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 within the hierarchy respond to goals and directions set in modules above it and to data and information presented from modules below it. 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.

The device network level consists of sensors, actuators, and communications links. The next highest level consists of control, surveillance, and diagnostic modules. The coupling of the control modules with the lower-level nodes is equivalent to an automated control system composed of controllers and field devices. The surveillance and diagnostic modules provide derived data to support condition determination and monitoring for components and process systems. The hybrid control level provides command and signal validation capabilities and supports prognosis of incipient failure or emerging component degradation (i.e., fault identification). The command level provides algorithms to permit reconfiguration or adaptation to accommodate detected or predicted plant conditions (i.e., active fault tolerance). For example, if immediate sensor failure is detected by the diagnostic modules and the corresponding control algorithm gives evidence of deviation based on command validation against preestablished diverse control algorithms, then the command module may direct that an alternate controller, which is not dependent on the affected measurement variable, be selected as principal controller. The actions taken at these lower levels can be constrained to predetermined configuration options

implemented as part of the design. In addition, the capability to inhibit or reverse autonomous control actions based on operator commands can be provided. The highest level of the autonomous control architecture provides the link to the operational staff.

IV.B. Framework for Autonomous Control Functionality

A variation on the nuclear plant supervisory control architecture and the CLARAty architecture for microrovers seems appropriate for consideration as the framework to support autonomy for a SRPS control system. Figure 2 illustrates the concept. Essentially, the approach of a hierarchical distribution of supervisory control and diagnostic functionality throughout the control system structure is adopted, while the overlaid decision functionality is maintained. It is possible to blend the decision and functional layers for this application domain because the planning regime for nuclear power system operation is much more restricted than for robotic or spacecraft applications. For example, while there are a multitude of paths that a robot may traverse as it navigates to its next site, the states are allowed for a SRPS are much more constrained. Even in the event of transients or faults, the control system will try to drive the plant back to a known safe state. This compression of the dual layers into a truncated three-sided pyramid allows for a deeper integration of control, diagnostics, and decision to provide the necessary capability to respond to rapid events and to adapt to changing or degraded conditions.

The granularity dimension is retained with more complexity shown at the lower hierarchical levels. Additionally, the information and command flow reflects granularity as well. At lower granularity, volumes of data are present. As the granularity increases moving up the hierarchy, the data are processed into system state and diagnostic/prognostic information that is subsequently refined into status and indicator information. On the command side, the transition from the top is demands to commands to control signals with the resolution of the plant/system control growing increasingly more detailed.

As with the supervisory control architecture, the bottom two levels of the hierarchy are the equivalent of an automated control system. The embedded functionality that enables a reliable, fault-tolerant implementation is indicated as a base intelligence. It is expected that there will be some decision capability associated with the control/surveillance/diagnostics level of that baseline system. The higher levels of the hierarchy assume greater degrees of decision capabilities.

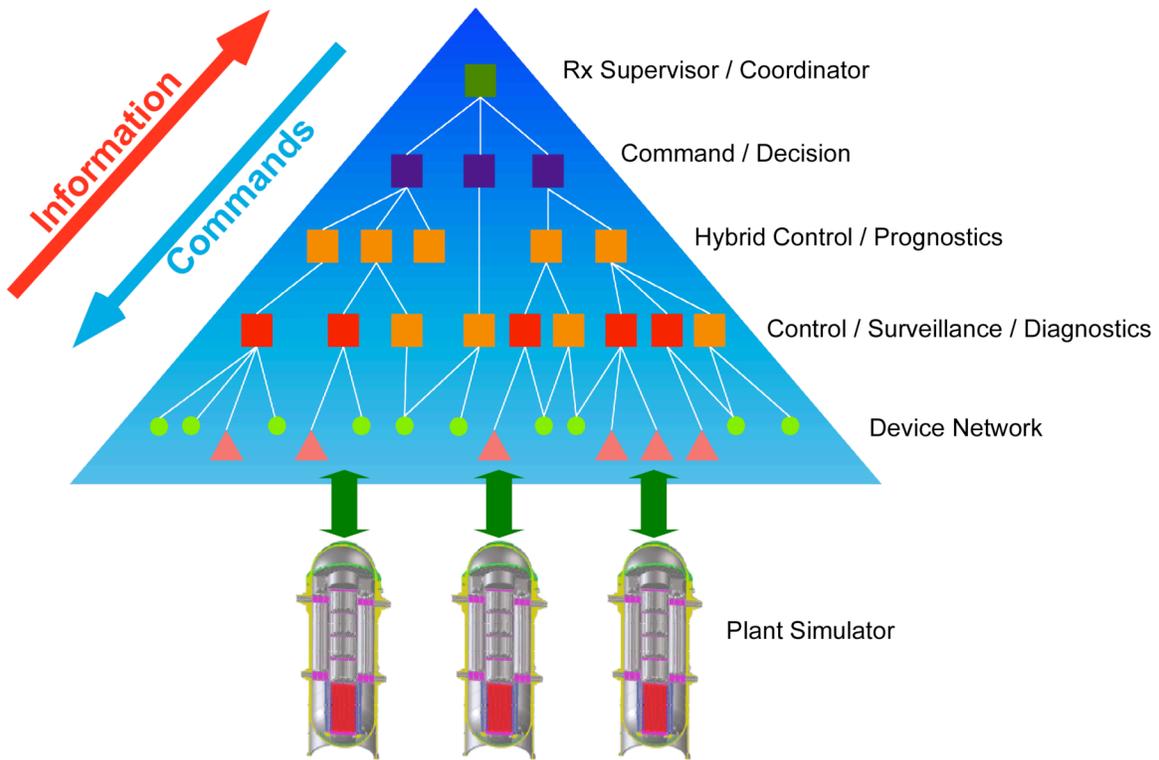


Fig. 1. Supervisory control architecture for multimodular nuclear power plants.

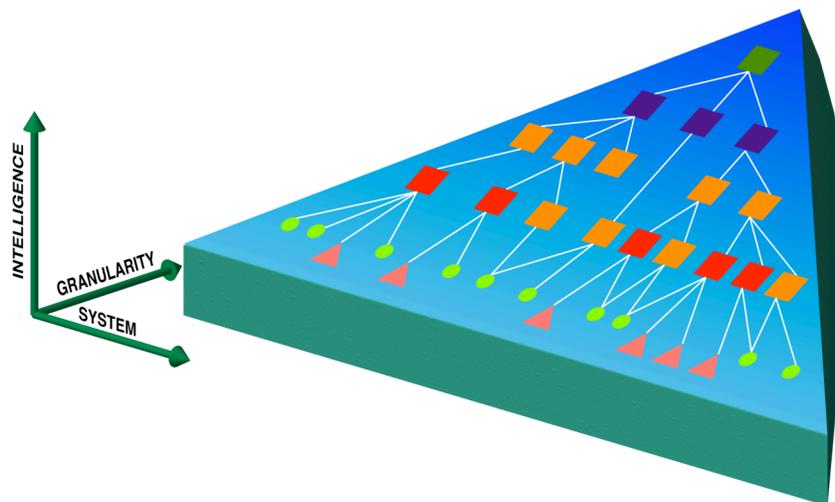


Fig. 2. Hierarchical framework to support SRPS control system autonomy.

In addition to the communications within the hierarchy, the autonomous control system must coordinate with the spacecraft control system and keep the mission control staff informed. To this end, the

reactor supervisor/coordinator node must communicate information about the status of the SRPS and the control system and also receive directives and commands. The information provided by the supervisor node can include

SRPS operational status and capability (e.g., constraints due to degradation), control action histories, diagnostic information, self-validation results, control system configuration, and data logs. Additional communication outside of the hierarchy may be required to coordinate control actions with other segments of the spacecraft, such as the power conversion system.

The functionality that is embodied in the hierarchy can be decomposed into several elements. These include data acquisition, actuator activation, validation, arbitration, control, limitation, checking, monitoring, commanding, prediction, communication, fault management, and configuration management. The validation functionality can address signals, commands, and system performance. The arbitration functionality can address redundant inputs or outputs, commands from redundant or diverse controllers, and status indicators from various monitoring and diagnostic modules. The control functionality includes direct plant or system control and supervisory control of the SRPS control system itself. The limitation functionality involves maintaining plant conditions within an acceptable boundary and inhibiting control system actions. The checking functionality can address computational results, input and output consistency, and plant/system response. The monitoring functionality includes status, response, and condition or health of the control system, components, and plant, and it provides diagnostic and prognostic information. The commanding functionality is directed toward configuration and action of lower level controllers and diagnostic modules. The prediction functionality can address identification of plant/system state, expected response to prospective actions, remaining useful life of components, and incipient operational events or failures. The communication functionality involves control and measurement signals to and from the field devices, information and commands within the control system, status and demands between the SRPS control system and spacecraft or ground control. The fault management and configuration management functionalities are interrelated and depend on two principal design characteristics. These are the ability of the designer to anticipate a full range of faults and the degree of autonomy enabled by the control system design.

Finally, the distribution of functions throughout the hierarchy must be established based on the degree of autonomy selected, technology readiness, reliability and fault management considerations, software development practices and platform capabilities, and the physical architecture of the SRPS control system hardware. Because an autonomous control system has never been implemented for a nuclear reactor and because several functional capabilities remain underdeveloped (as seen in the overview of the state of the art), there is clearly a

critical need for further development and demonstration of a suitable architectural framework.

V. CONCLUSIONS

The control system for a SRPS will be subject to unique challenges as compared to terrestrial nuclear reactors, which employ varying degrees of human control and decision-making for operations and benefit from periodic human interaction for maintenance. In contrast, the SRPS control system must be able to provide continuous, remote, often-unattended operation for a mission lasting a decade or more with limited immediate human interaction and no opportunity for hardware maintenance. In addition to the inaccessibility and periods of unattended operation, the SRPS control system must accommodate severe environments, system and equipment degradation or failure, design uncertainties, and rare or unanticipated operational events during an extended mission life. As a result, the capability to respond to rapid events and to adapt to changing or degraded conditions without near-term human supervision is required to support mission goals. Autonomous control can satisfy essential control objectives under significant uncertainties, disturbances, and degradation without requiring any human intervention. Therefore, autonomous control is necessary to ensure the successful application of a SRPS for deep space missions.

Key characteristics that are feasible through autonomous control include

- intelligence to confirm system performance and detect degraded or failed conditions,
- optimization to minimize stress on SRPS components and efficiently react to operational events without compromising system integrity,
- robustness to accommodate uncertainties and changing conditions, and
- flexibility and adaptability to accommodate failures through reconfiguration among available control system elements or adjustment of control system strategies, algorithms, or parameters.

Autonomous control must be addressed early in the design of the SRPS to determine the degree of autonomy required. Mission requirements, design trade-offs, and the state of the technology will affect the autonomous capabilities to be included. The extent to which the key characteristics of autonomy are realized depends on the level of responsibility that is to be entrusted to the autonomous control system. Given anticipated mission imperatives to utilize technology with demonstrated (or at least high probability) readiness, it is not practical to strive for the high-end extreme of autonomy. Instead, modest advancement beyond fully automatic control to

allow extended fault tolerance for anticipated events or degraded conditions and some predefined reconfigurability is the most realistic goal for an initial application of SRPS autonomous control. A hierarchical functional architecture providing integrated control, diagnostic, and decision capabilities that are distributed throughout the hierarchy can support this approach.

Control systems with varying levels of autonomy have been employed in robotic, transportation, spacecraft, and manufacturing applications. However, autonomous control has not been implemented for an operating terrestrial nuclear power plant. Therefore, technology development and demonstration activities are needed to provide the desired technical readiness for implementation of a SRPS autonomous control system. In particular, the capabilities to monitor, trend, detect, diagnose, decide, and self-adjust must be established to enable control system autonomy. Finally, development and demonstration of a suitable architectural framework is also needed.

ACKNOWLEDGMENTS

This work was performed under the sponsorship of NASA's Project Prometheus and directed by DOE/NNSA Naval Reactors. Opinions and conclusions drawn by the author are not endorsed by DOE/NNSA Naval Reactors.

REFERENCES

- [1] P. J. ANTSAKLIS and K. M. PASSINO, "An Introduction to Intelligent Autonomous Control Systems with High Degrees of Autonomy," *An Introduction to Intelligent and Autonomous Control*, pp. 1-26, Kluwer Academic Publishers, Boston (1992).
- [2] K. J. ASTROM, "Toward Intelligent Control," *IEEE Control System Magazine*, 60-64 (April 1989).
- [3] T. R. CHAUDHURI et al., "From Conventional to Autonomous Intelligent Methods," *IEEE Control System Magazine*, 78-84 (October 1996).
- [4] K. M. PASSINO, "Intelligent Control for Autonomous Systems," *IEEE Spectrum*, 55-62 (June 1995).
- [5] B. P. ZEIGLER and S. CHI, "Model Based Architecture Concepts for Autonomous Control Systems Design and Simulation," *An Introduction to Intelligent and Autonomous Control*, pp. 57-78, Kluwer Academic Publishers, Boston (1992).
- [6] H. BASHER and J. S. NEAL, *Autonomous Control of Nuclear Power Plants*, ORNL/TM-2003/252, Oak Ridge, Oak Ridge National Laboratory (2003).
- [7] *Proceedings of the 1993 ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, Oak Ridge, April 1993, American Nuclear Society (1993).
- [8] *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 96)*, Vols. 1 and 2, State College, Pa., May 1996, American Nuclear Society (1996).
- [9] *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, Washington D.C., November 2000, American Nuclear Society (2000).
- [10] *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2004)*, Columbus, September 2004, American Nuclear Society (2004).
- [11] A. G. MISHKIN et al., "Experiences with Operation and Autonomy of the Mars Pathfinder Microover," *Proceedings of the 1998 IEEE Aerospace Conference*, Aspen, March 1998, pp. 337-351, Institute of Electrical and Electronics Engineers (1998).
- [12] R. VOLPE et al., "The CLARAty Architecture for Robotic Autonomy," *Proceedings of the 2001 IEEE Aerospace Conference*, Big Sky, Mont., March 2001, Vol. 1, pp. 121-131, Institute of Electrical and Electronics Engineers (2001).
- [13] M. D. RAYMAN et al., "Results from the Deep Space 1 Technology Validation Mission," *Proceedings of the 50th International Astronautical Congress*, American Institute of Aeronautics and Astronautics, *Acta Astronautica*, 47, 475-488 (1999).
- [14] R. W. WINKS, T. L. WILSON, and M. AMICK, "B&W PWR Advanced Control System Algorithm Development," *Proceedings: Advanced Digital Computers, Controls, and Automation Technologies for Power Plants*, EPRI TR-100804, Palo Alto, Electric Power Research Institute (1992).
- [15] R. ALAMI et al., "An Architecture for Autonomy," *International Journal of Robotics Research*, 17(4), 315-337 (1998).
- [16] E. GAT, "Three-Layer Architectures," *Artificial Intelligence and Mobile Robots: Case Studies of Successful Robot Systems*, pp. 195-210, D. KORTENKAMP et al., Eds., MIT Press, Cambridge (1998).
- [17] R. T. WOOD et al., "Autonomous Control for Generation IV Nuclear Plants," *Proceedings of the 14th Pacific Basin Nuclear Conference*, Honolulu, March 2004, pp. 517-522, American Nuclear Society (2004).