Autonomous Control for Generation IV Nuclear Plants

R. T. Wood
Oak Ridge National Laboratory
P.O. Box 2008, MS 6010
Oak Ridge, Tennessee 37831
E-mail: woodrt@ornl.gov

C. Ray Brittain
Oak Ridge National Laboratory
P.O. Box 2008, MS 6010
Oak Ridge, Tennessee 37831
E-mail: brittaincr@ornl.gov

Jose March-Leuba
Oak Ridge National Laboratory
P.O. Box 2008, MS 6010
Oak Ridge, Tennessee 37831
E-mail: marchleubaja@ornl.gov

James A. Mullens
Oak Ridge National Laboratory
P.O. Box 2008, MS 6010
Oak Ridge, Tennessee 37831
E-mail: mullensja@ornl.gov

John S. Neal
Oak Ridge National Laboratory
P.O. Box 2008, MS 6010
Oak Ridge, Tennessee 37831
E-mail: nealjs1@ornl.gov

Abstract—*Several Generation IV nuclear reactor concepts have goals for optimizing investment recovery through phased introduction of multiple units on a common site with shared facilities and/or reconfigurable balance-of-plant systems. Additionally, these concepts promote significant reductions in plant operations and maintenance staff. To accomplish these goals, intelligent control and diagnostic capabilities are needed to provide nearly autonomous operations with anticipatory maintenance. A fully autonomous control system should enable automatic operation of a nuclear plant while adapting to equipment faults and other upsets. It needs to have many intelligent capabilities, such as diagnosis, modeling, analysis, planning, reconfigurability, self-validation, and decision. These capabilities have been the subject of research for many years but a fully autonomous control system remains an as-yet unrealized goal. This paper describes a functional framework for intelligent, autonomous control that can facilitate the integration of control, diagnostic, and decision-making capabilities to satisfy the operational and performance goals of next-generation modular nuclear power plants.*

I. INTRODUCTION

Nuclear plants of the 21st century will employ higher levels of automation and fault tolerance to increase availability, reduce accident risk, and lower operating costs. Key developments in control algorithms, fault diagnostics, fault tolerance, and communications for distributed systems are needed to implement fully automated plants. Equally challenging will be integrating developments in separate information and control fields into a cohesive system, which collectively achieves the overall goals of improved performance, safety, reliability, maintainability, and cost-effectiveness. Several Generation IV nuclear reactor concepts have goals for optimizing investment recovery through phased introduction of multiple units on a common site with shared facilities and/or reconfigurable balance-of-plant systems. Additionally, these concepts promote significant reductions in plant operations and maintenance staff.

To accomplish the goals of next-generation nuclear power plants, intelligent control and diagnostic capabilities are needed to provide nearly autonomous operations with anticipatory maintenance. Autonomous control can satisfy essential control objectives under significant uncertainties, disturbances, and degradation without requiring immediate human intervention. Characteristics and capabilities of autonomous control systems have been studied and control systems with varying levels of autonomy have been employed in robotic, transportation, spacecraft, and manufacturing applications.[1-4] However, autonomous control has not been implemented for an operating nuclear power plant. Nevertheless, important considerations for achieving autonomous or intelligent control for nuclear power systems have been proposed and recent research efforts within the nuclear power community have addressed several building blocks for autonomy.[5, 6]

A fully autonomous control system should enable automatic operation of a nuclear plant while adapting to equipment faults and other upsets. It needs to have many intelligent capabilities, such as diagnosis, modelling, analysis, planning, reconfigurability, self-validation, and decision. These capabilities have been the subject of research for many years but a fully autonomous control system remains an as-yet unrealized goal. This paper describes a functional framework for intelligent, autonomous control that can facilitate the integration of control, diagnostic, and decision-making capabilities to satisfy the operational and performance goals of modular power plants.

II. SUPERVISORY CONTROL FRAMEWORK

To fully achieve the economic benefits of multi-unit Generation IV nuclear plants, it will be desirable to have a limited operations and maintenance staff. The combined factors of a reduced operating crew and more complex dynamics means a different approach is needed for overall control of the plant. One element of the solution is to develop a supervisory control system. The role of a supervisory control system is to act as an extension of the human operator to assure safe, reliable operation of the plant. The supervisory control system provides the framework for integrating algorithm-based controllers and diagnostics at the subsystem level with command and decision modules at higher levels. The higher levels of the functional hierarchy are where the supervisory control system provides autonomous capabilities while accommodating the human operator's analytical approach and need to be cognizant of the state of the plant. This approach provides the framework for autonomous control while supporting a high-level interface with the operating crew, 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 supervisory control structure envisioned for multi-unit Generation IV nuclear reactors, pictured in Figure 1, is hierarchical with a recursive nature. Each node in the hierarchy (except for the terminal nodes at the base) is a supervisory module. The supervisory control module at each level responds 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 and necessary supporting information to functionally-connected modules.

In addition to the communications up and down the hierarchy, the supervisory controller must keep the operator informed about the status of the plant. To this end, the supervisory controller must communicate information about the status of the plant, any data needed to support the information, any impending control actions, the reason for the control action, and the expected result of the action. The goal of this communication is to assure the operator is well informed about the status of the plant and the control system. The operator must have confidence that the plant is in a safe state and that the control system is functioning to keep the plant operational while meeting both short term and long term goals. The human operator has the opportunity to interact and direct the goals and actions of the supervisory controller. This interaction may take place directly with any module in the hierarchy. Examples of such interaction include setting plant power output goals and unit demands, interrogating prognostics modules about trends in component health, and applying manual control of individual control loops. This capability assures that the human operator can assume ultimate responsibility for the safety and operation of the plant.

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

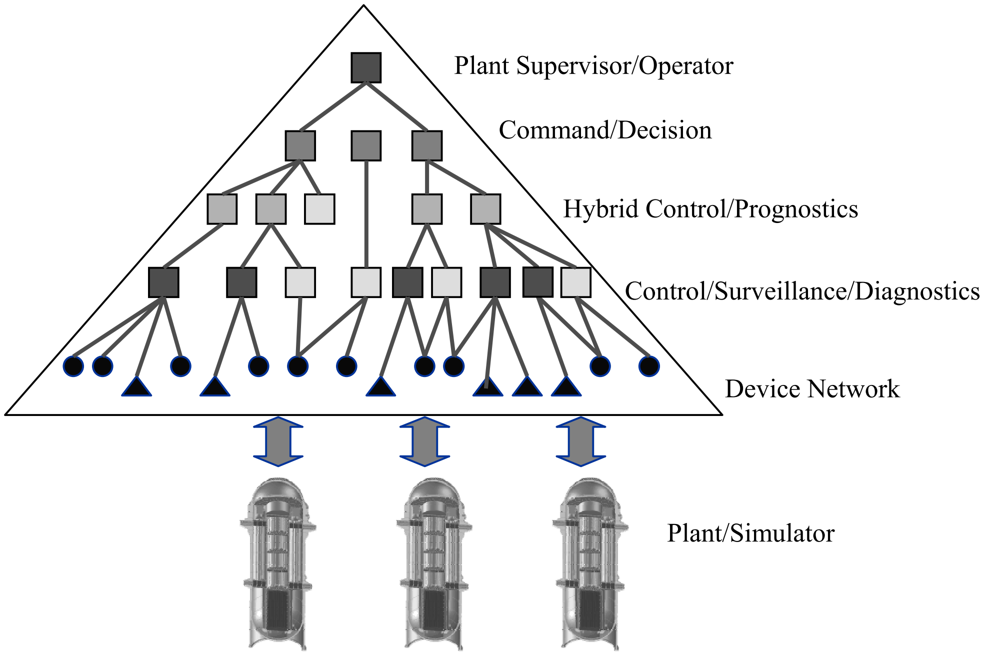

FIGURE 1. A Hierarchical Framework for Supervisory Control of a Multi-Modular Plant

lower-level nodes is equivalent to an automatic 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. At this level, fault identification occurs. The command level provides algorithms to permit reconfiguration or adaptation of the control system to accommodate detected or predicted plant conditions. At this level, active fault tolerance is accomplished. 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 pre-established 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 through operator intervention is available. The highest level of the functional architecture provides the interface to the operations staff. An informational interface to the maintenance staff can supply component and device health status information to permit optimized, "just-in-time" maintenance scheduling.

III. SELF-VALIDATING CONTROL ENGINE

The foundation for autonomous control should begin early in the design phase of an advanced nuclear plant. The control system design for multi-modular Generation IV nuclear power plants can build on recent advances in control theory. Specifically, methods are available for automated generation of the control system which can be traced directly to the design requirements throughout the life of the plant. Implementation of these methods can capture the design requirements inside a control engine during the design phase. This control engine will not only be capable of automatically designing the initial implementation of the control system, but it also can confirm that the original design requirements are still met during the life of the plant as conditions change.

An automatic control design technology has been developed under a Nuclear Energy Research Initiative project for the U.S. Department of Energy.[7] The result is a control engine that can be used during the design phase for automatic generation of a control system and then implemented as part of the control structure to permit periodic confirmation of the control system performance. Because the control engine captures the functional requirements used to define the design, the self-validation results can be traced directly to the technical basis for the control system at any point during the life of the system.

As described in reference 7, the control engine captures the high-level requirements and stress factors that the control system must survive (e.g., a list of transients or a requirement to withstand a single failure). This is accomplished by reformulating the performance requirements as mathematical constraints of a minimization problem. For example, one such constraint could be that the reactor T-average control system must respond to an anticipated over-cooling event without scram. Given the captured requirements, the control engine is able to subsequently generate the control-system algorithms and parameters that optimize a design goal and satisfy all requirements. Essentially, the design requirements are fed into a control engine, which uses a library of control algorithms and validated plant models to arrive at the control design based on an iterative optimization process. The control design is then implemented using validated control architectures, which are tested automatically to guarantee that the reliability requirements are met. Finally, diagnostics are developed to help maintain an accurate the plant model (e.g., the model can be updated with component failures or mode changes) for subsequent control design and evaluation.

The implementation of this control-engine design methodology requires the following steps (see Figure 2):

1) Determination of design requirements related to control system performance,
2) Representation of requirements in mathematical form,
3) Access to (or development of) a control algorithm library,
4) Development and validation of plant models,
5) Automated control design generation,
6) Evaluation of control architectures,
7) Control design implementation, and
8) Implementation (or development) of diagnostics methods to update the plant model.

In addition to automatically designing the initial implementation of the control system, the control engine also can be used to confirm that the original design requirements are still met during the life of the plant as conditions change (e.g., component degradation or subsystem failures). Implementation of the control engine as part of a self-validating structure is illustrated in Figure 3. The control engine runs in the background in supervisory mode and continuously evaluates whether all requirements and constraints are satisfied given the current state of the plant. The state of the plant is represented by validated plant models. As diagnostic modules detect degradation (e.g., sensor drift or actuator sticking) or component failure, the plant simulation

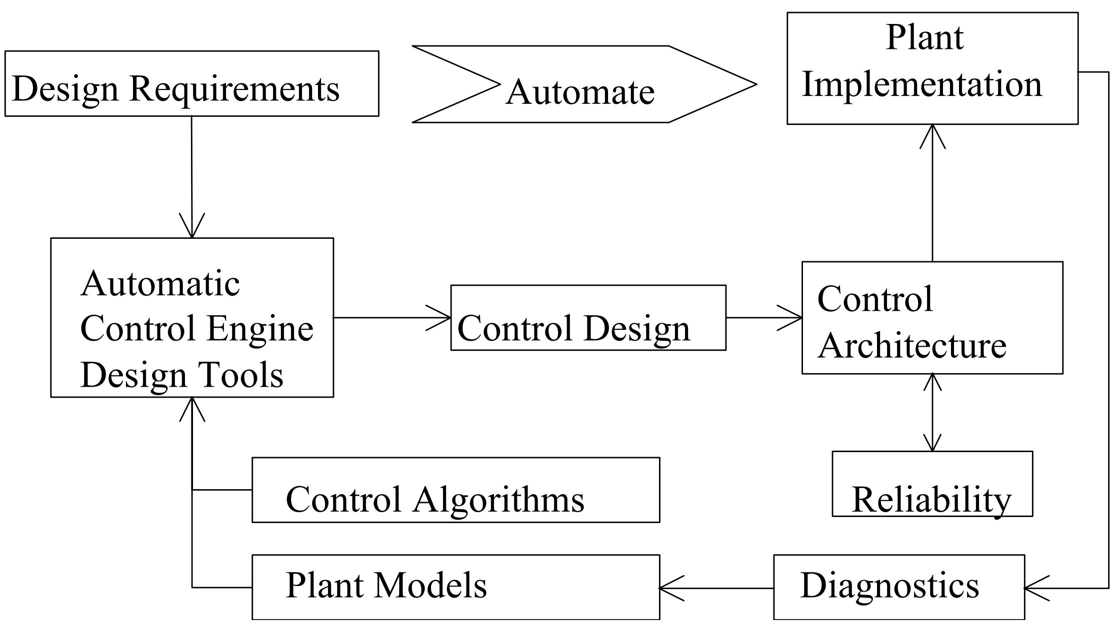

FIGURE 2. Schematic Diagram of the Automated Control Design Process

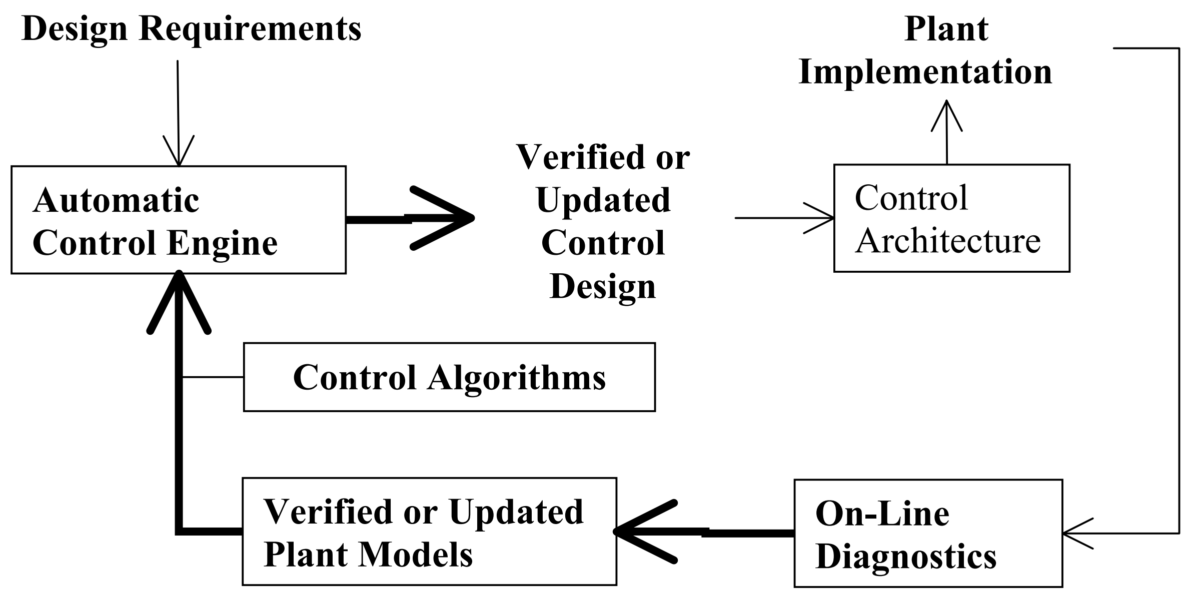

Figure 3. Illustration of Self-Validating Control System Structure Employing Automatic Control Engine

models are automatically updated using adjusted parameters and module switching. When the plant condition undergoes sufficient changes to result in inability of the control system to satisfy one or more of the design requirements, the control engine starts an iterative minimization calculation that determines optimal control parameter settings or even different control strategies if the current one is inadequate. Since most changes to the plant over its 60 year life are slow in nature, it is not envisioned that the control engine would function in a closed loop by automatically changing control parameters or strategies. Its function would be more of an advisory nature through generation of an alert when the original control-system performance requirements are not satisfied under the present conditions (e.g., hardware failures or plant reconfiguration). In addition to the alert, the control engine can also suggest new control system settings that would satisfy the performance requirements under the present plant condition.

It should also be noted that the self-validating controller structure can be easily implemented at higher levels of the supervisory control architecture. By building in appropriate diagnostics and including high-fidelity simulation models that can be automatically updated, the autonomous control system can determine when subsystem performance has degraded to the point of possibly violating design goals. After the degradation has been diagnosed, the operations and maintenance staff can be notified and authorized corrective action can be taken by the autonomous control system through reconfiguration among pre-designed options.

IV. CONCLUSIONS

The architectural framework presented in this paper provides the foundation of an autonomous control system for a Generation IV multi-modular plant. The hierarchical supervisory control structure can support full integration of control, diagnostic, and decision modules to provide a high degree of automation and the basis for expanded autonomy in operations. In addition, an autonomous control system can provide the capability for self-validation and adaptation throughout extended operational periods over the plant lifetime. Properly implemented, autonomous control can contribute the following characteristics to a Generation IV control system:

- intelligence to confirm system performance and detect degraded or failed conditions,
- optimization to minimize stress on plant 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.

However, autonomous control has not yet been applied to an operating nuclear power plant. Thus, fulfilling the promise of autonomous control to achieve the goals of Generation IV reactor concepts requires the development and demonstration of several innovative structures and technical capabilities. In effect, a comprehensive development program is needed. Areas of research that should be considered in establishing such a program include fault management and reliability assessment methodologies, software dependability assessment techniques (e.g., software reliability quantification), system diagnostics and component prognostics, intelligent control and decision algorithms and human cognition and the role of the operator.

REFERENCES

1. P.J. Antsaklis and K.M. Passino, *An Introduction to Intelligent and Autonomous Control*, Kluwer Academic Publishers, Boston, 1992.
2. K.J. Astrom, "Toward Intelligent Control," *IEEE Control System Magazine*, April 1989.
3. T.R. Chaudhuri, L.G.C. Hamey, and R.D. Bell, "From Conventional to Autonomous Intelligent Methods," *IEEE Control System Magazine*, October 1996.
4. K.M. Passino, "Intelligent Control for Autonomous Systems," *IEEE Spectrum*, June 1995.
5. H. Basher and J.S. Neal, *Autonomous Control of Nuclear Power Plants*, ORNL/TM-2003/252, Oak Ridge National Laboratory, Oak Ridge, Tennessee (October 2003).
6. R.E. Uhrig, "Opportunities for Automation and Control of the Next Generation of Nuclear Power Plants," *Nuclear Technology*, **88**, 1989, pp. 157-165.
7. J.A. March-Leuba and R.T. Wood, "Development of an Automated Approach to Control System Design," *Nuclear Technology*, **141**, 2003, pp. 45-53.