ORNL/SPR-2019/1178
M2CT-19OR06090137

Transformational Challenge Reactor Autonomous Control System Framework and Key Enabling Technologies

Sacit M. Cetiner
Pradeep Ramuhalli

May 31, 2019

**Approved for public release.
Distribution is unlimited.**

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

ORNL/SPR-2019/1178
M2CT-19OR06090137

Transformational Challenge Reactor (TCR) Program

TRANSFORMATIONAL CHALLENGE REACTOR AUTONOMOUS CONTROL SYSTEM FRAMEWORK AND KEY ENABLING TECHNOLOGIES

Author(s)
Sacit M. Cetiner
Pradeep Ramuhalli

Date Published: May 31, 2019

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

EXECUTIVE SUMMARY

Autonomous operation may offer the potential to significantly improve the economics of nuclear power plants while maintaining operation within the safety envelope of the reactor. If developed and deployed, autonomous operation technology may enable deployment of small reactors at remote sites while minimizing the requirements of operator support. Within the context of the Transformational Challenge Reactor (TCR) program, autonomous control along with the other unique characteristics of the reactor is expected to enable cost-effective nuclear energy systems.

This document describes a framework for enabling autonomy for nuclear energy systems, and describes key enabling technologies including embedded sensing. Autonomous control, when combined with the enhancements offered by advanced manufacturing methods, is expected to play a key role in restoring the economic viability of nuclear power generation.

For regulatory acceptance, autonomous microreactors will most likely need to demonstrate a high degree of passive safety and a small source term. Such attributes will allow a minimal emergency plan, which could lead to reduced onsite staffing and will potentially allow a remotely located control room. Highly autonomous reactor designs must consider technical specifications (TSs) regarding design safety limits, limiting safety settings, and limiting control settings. An autonomous reactor design must operate the reactor according to TS guidelines, provide for appropriate equipment surveillance, and provide acceptable record-keeping and other administrative controls. Moreover, highly autonomous reactor designs will interface directly with safety-related and important-to-safety systems and functions, and will need to account for cybersecurity considerations to demonstrate adequate protection of the health and safety of the public and the environment.

Advanced feedback controls and autonomous controls are observed in many engineering disciplines—from deep space missions, unmanned aerial vehicles to self-driving cars. Nuclear power generation is lagging behind other process industries in adopting the advances that have emerged in the last two decades. While these domains have differences in the requirements for autonomous operation, they can offer insights into the construction of a proper framework and functional architecture for autonomous operations in a nuclear power plant.

Decision-making is the foundational function for autonomy. One of the basic human cognitive processes, it is the selection of a preferred option, or a course of actions, from a set of alternatives based on certain criteria. Mathematically, decision-making is a problem-solving activity to identify and analyze the available courses of actions and to determine the most appropriate option given the set of conditions and constraints.

While search based algorithms such as those that rely on Bellman's *principle of optimality* provide a more realistic situational analysis, and hence awareness, implementation of these algorithms in industrial problems is limited and therefore poses a risk for the aggressive schedule of the TCR program. Decision-making and supervisory control models based on discrete event systems—either finite state automata or Petri nets—have an established industrial track record, with applications ranging from robotics to self-driving cars. Based on this observation, it can be concluded that finite state machine formalism offers the best approach for implementation of the TCR autonomous control system.

A typical nuclear plant I&C system includes three major subsystems: (1) Reactor Protection System (RPS), (2) Plant Control System (PCS), and (3) Data Communication System (DCS). The approach for the TCR I&C system design will minimize potential regulatory challenges for implementation of the I&C platform. This will be accomplished by relying on approved components and systems that have safety or safety-related functions—to the extent possible. For non-safety–related controls (i.e., the plant control

system and other ancillary controls), more advanced control approaches can be adopted if they have sufficient industrial pedigree.

TCR will adopt a three-layer autonomous control architecture: (1) functional layer, (2) coordination layer, and (3) organization layer. The functional layer of the TCR autonomous control system architecture deals with low-level control functions including classical feedback control. The coordination layer of the TCR autonomous control system includes an implementation of the finite state machine to perform higher level control functions. Operating modes and the associated mode transitions are the standard means of achieving plant startup and shutdown. These modes and transitions are highly proceduralized, labor intensive and time-consuming activities.

The finite state machine approach is preferred for this layer as it offers a balance between performance and risk. Finite state machines are well-suited for mathematical representation of complex engineering procedures. The rich mathematical foundation available from automata theory also provides confidence for testability and qualification. For instance, the regular language formalism of a supervisory control system exploits the best features of *regular expressions*. This provides a compact, *finite* representation for potentially complex languages with an infinite number of strings.

The organization layer of the TCR autonomous control system is reserved for more complex decision-making algorithms that rely on search-based methods such as dynamic programming. Currently, no decision has been made regarding the implementation details of this layer.

Autonomous control implies decision-making, and decision-making requires an abundance of data to make informed decisions. However, small-size reactor cores such as that of the TCR do not allow copious internal space to allow placement of large quantities of sensors. Therefore, for additional data from the core, embedded sensing emerges as a natural solution. Embedded sensing would prevent undesired obstructions in the internal flow path and would help realize the true benefits of an additively manufactured core.

Three measurement modalities stand out in the short term for embedded sensing: (1) embedded temperature sensing, (2) embedded strain sensing, and (3) embedded neutron flux and/or gamma field sensing. Additionally, distributed monitoring of structural vibration and coolant flow may offer significant advantages.

Data analytics technologies are considered an enabling technology for autonomous control and operation. Essential data analytics and control technologies for the first TCR demonstration include online monitoring for sensor drift, as well as SSC diagnostics for plant state and control actuation confirmation.

This report offers the following key takeaways pertinent to our control strategy for TCR and demonstration of relevant, yet achievable advances towards autonomous nuclear energy systems: (1) discrete event models based on finite state machine models offer the best near-term approach for the implementation of the TCR autonomous control system, (2) the TCR I&C system design will adopt an approach that minimizes potential regulatory challenges, (3) it will rely on endorsed components and systems that have safety or safety-related functions.

CONTENTS

Page

ABSTRACT

This document describes a framework for enabling autonomy for the nuclear energy systems, and describes key enabling technologies including embedded sensing. Autonomous control, when combined with the enhancements offered by advanced manufacturing methods, is expected to play a key role in restoring the economic viability in nuclear power generation.

TCR will adopt a three-layer autonomous control architecture: (1) functional layer, (2) coordination layer, and (3) organization layer. The coordination layer forms the foundation of the autonomous control system; it performs higher level control functions through the implementation of a finite state machine. Autonomous plant startup and shutdown procedures were selected as the primary demonstration target. Operating modes and the associated mode transitions are the standard means of achieving these plant transients. These modes and transitions are highly proceduralized, labor intensive and time-consuming activities. Finite state machines are capable for mathematical representation of complex engineering procedures and are the preferred solution for this layer.

Autonomous control implies decision-making, and decision-making requires abundance of data. Embedded sensing is considered as a potential solution. Three measurement modalities stand out in the short term for embedded sensing: (1) embedded temperature sensing, (2) embedded strain sensing, and (3) embedded neutron flux and/or gamma field sensing. Additionally, distributed monitoring of structural vibration and coolant flow may offer significant advantages.

Data analytics technologies are considered an enabling technology for autonomous control and operation. Essential data analytics and control technologies for the first TCR demonstration include online monitoring for sensor drift, as well as SSC diagnostics for plant state and control actuation confirmation.

ACRONYMS

AFSM	augmented finite state machine
AI	artificial intelligence
ALMR	Advanced Liquid Metal Reactor
AM	additive manufacturing
AOO	anticipated operational occurrence
ASIC	application-specific integrated circuits
CAN	controller area network
CLARAty	Coupled-Layer Architecture for Robotic Autonomy
DBE	design basis event
DCS	Data Communication System
DDP	differential dynamic programming
DES	discrete event systems
DOE	US Department of Energy
DoD	US Department of Defense
DP	dynamic programming
EBR	Experimental Breeder Reactor
ERL	Electronics Research Laboratory
ESA	electric signature analysis
EXEC	Smart Executive
FFTF	Fast Flux Test Facility
FIFO	first-in-first-out
FPGA	field-programmable gate array
FSV	Fort St. Vrain
GPS	global positioning system
GRG	generalized reduced gradient
HAD	highly autonomous driving
HTGR	high-temperature gas-cooled reactor
HX	heat exchanger
ICS	integrated control system
IE	initiating event
IRIS	International Reactor Innovative and Secure
LIDAR	light detection and ranging
LQG	linear quadratic Gaussian
LWR	light water reactor
MDP	Markov decision process
MER	Mars Exploration Rover
MIR	Mode Identification and Reconfiguration
MIMO	multiple-input multiple-output
MM	mission manager
NPAR	Nuclear Plant Aging Research
NP-hard	nondeterministic polynomial-time hard
NPP	nuclear power plant
NRC	US Nuclear Regulatory Commission
OLM	online monitoring
ORNL	Oak Ridge National Laboratory

PCS	power conversion system
PI	proportional-integral
PLC	programmable logic controllers
POMDP	partially observable Markov decision process
PRA	probabilistic risk assessment
P/S	planner/scheduler
RA	remote agent
RPS	Reactor Protection System
RTS	Reactor Trip System
SSC	structures, systems, and components
SFR	sodium-fast reactors
SISO	single-input single-output
SNR	signal-to-noise ratio
SPA	sense-plan-act
SPE	sense-plan execute
SPND	self-powered nuclear detector
SPGD	self-powered gamma detector
SQP	sequential quadratic programming
TCR	Transformational Challenge Reactor
TRL	technology readiness level
TS	technical specification
UAV	unmanned aerial vehicle
WRM	wide-range monitor

1. INTRODUCTION

Autonomous operation of nuclear plants has the potential to significantly improve the economics of existing plants while maintaining operation within the safety envelope of the reactor. If properly developed and deployed, autonomous operation technology may enable deployment of small reactors at remote sites while minimizing the requirements of operator support, and maintaining the health and safety of the public. In addition to reducing costs, the technology can add layers of safety by allowing for rapid decision making and actuation in off-normal situations.

Within the context of the Transformational Challenge Reactor (TCR) program, autonomous control along with the other unique characteristics of the reactor (advanced manufacturing) is expected to enable cost-effective nuclear energy systems. On the other hand, technology for autonomy can add risk if not properly developed. There is therefore a need for systematic development and demonstration of autonomy technology for TCR control.

This document describes a framework for enabling autonomy for the nuclear energy systems. It defines autonomous operation and examines whether autonomy is possible for nuclear systems. The report also describes enabling sensing technologies for autonomy and describes a framework to facilitate autonomy. In order to allow for detailed analysis and discussions, the TCR control system is specifically considered for autonomous operation.

1.1 BACKGROUND

The fundamental safety function of the structures, systems and components (SSCs) in a nuclear power plant (NPP) is to maintain proper rate of heat rejection from the core under all operating modes. To provide defense-in-depth, NPPs are designed with alternative heat rejection systems to guarantee that the core heat can be delivered to an ultimate heat sink. However, only the path through the power conversion system (PCS) can generate electricity. In order to maximize profitability, maximizing capacity factor and adapting power levels as demand changes are essential.

In an advanced (micro) reactor such as TCR, automating operational mode changes can increase economic efficiencies. The use of autonomous control systems for this purpose can further improve efficiencies by reducing manpower requirements while not compromising safety.

The nuclear power industry lags far behind other industries (e.g., aerospace, automotive, communications) in transferring the current human-based roles and responsibilities to machines, systems, and controls. Efforts focused in the research community have been limited to capturing expert knowledge and emulating human cognition, which often still requires some degree of local, active human supervision and intervention. Significant R&D is necessary to move beyond this like-for-like replacement to take advantage of the autonomous decision-making capabilities supported by deliberate, high degrees of system integration and automation.

Automation and *autonomy* are two different concepts. *Automation* refers to a predetermined action or set of actions to reach a desired state given a condition or change in condition. Automation is widely used in almost every facet of our lives; it is merely a convenience to perform a series of tasks following a trigger. In an automated process, all input states are assumed known. Hence, uncertainties in monitored processes, unforeseen system states, or deteriorating conditions cannot be treated explicitly.

Autonomy, on the other hand, is the ability of a system to determine and perform necessary tasks without human intervention. *Decision-making*, including *reasoning*, is the fundamental tenet of autonomy. Interest in autonomous systems has gained momentum with deep space missions, where timely intervention for course correction from the Earth clearly would not be conceivable. Recently, with technological advances and interest in autonomous driving, complex decision-making algorithms are receiving increased attention.

Autonomy should never be perceived as a plug-and-play capability. On the contrary, it is a product of a highly complex systems engineering process that clearly defines the functions expected from the control system and the allocation of such functions between the autonomous system and human operators.

Autonomous systems require integration of control systems with operator decision support technology. Some critical aspects of the this technology are (1) the integration of online monitoring with the interpretation of the plant's state, (2) generation of an operational strategy during a plant upset condition, and (3) assessment of risk associated with proposed actions based on the trajectory between current and postulated plant states. Without a technically sound framework for achieving this outcome, significant staff reduction will continue to be a challenge.

The primary gap in achieving this vision relates to autonomous decision-making capabilities that are strategic, interpretive, adaptive, and predictive.[1] To date, automation of operations and maintenance (O&M) planning at nuclear facilities has been limited to time-based activities with some small degree of anticipatory coordination. Equipment surveillance, diagnostics, and prognostics have been used for offline asset management and modest decision support, but these technologies are not being fully leveraged for intelligent, optimal O&M planning and control. Application of these advanced capabilities based on highly integrated digital technologies can support real-time autonomous decision-making within an advanced control and diagnostics framework. This level of self-cognition is necessary to support the realization of truly autonomous nuclear power generation, particularly in remote locations where infrastructure is limited. To achieve the desired operational efficiency with a reduced staffing burden, autonomous decision-making must be developed and demonstrated in the nuclear power context.

It is recognized that once an operator is out of the control loop, his or her understanding or mental picture of the plant is not maintained, presenting problems when he or she is required to participate. This results in resistance to automating the plant to the maximum extent possible, as well as reluctance to minimizing the operator's involvement in plant control. To help the operator in maintaining an understanding of the plant, comprehensive information is provided in the main control room in a clear, readily assimilable form via mimics of the plant on hard panels and computer-based displays.[2] Therefore, any autonomous control framework must be developed holistically within a sound *concept of operations* framework where the implications of human-automation collaboration are analyzed in an integral manner.

As nuclear plants become smaller, the cost per megawatt of electricity increases, with the bulk of this cost being attributed to O&M activities.[3] The increased interest in small reactors (<300 MWe) and micro-reactors (<20 MWe) has resulted in a recent incentive to examine and develop autonomous operation technologies further. Additional sensors, instrumentation, and advances in control room displays are expected to help maintain operator awareness of the plant state under these conditions.

[1] S. M. Cetiner, et al., "Technical Basis for Automated Decision Making: a Survey on the State-of-the-art of Decision Making and Existing Analytical Tools," ORNL/LTR-2014/26, Oak Ridge National Laboratory, Oak Ridge, TN (2014).
[2] IAEA-TECDOC-668, "The Role of Automation and Humans in Nuclear Power Plants," International Atomic Energy Agency (1992).
[3] "Nuclear Costs in Context," White Paper, Nuclear Energy Institute, Washington, DC (April 2017).

1.2 REGULATORY CONSIDERATIONS FOR AUTONOMY

A recent report published by Oak Ridge National Laboratory (ORNL) describes an investigation of the regulatory implications of autonomous control of nuclear reactors, with a focus on microreactors.[4] While the report puts emphasis solely on power reactors, with the US Nuclear Regulatory Commission (NRC) as the licensing authority, it captures potential challenges that may arise unless requirements are properly addressed. This report provides a brief summary of the conclusions and recommendations from the report.

The primary path for the licensing and regulation of US-based power reactors is through the NRC. This is because, by statute, the US Department of Energy (DOE) and the US Department of Defense (DoD) are not currently positioned to license power reactors, although DoD could be authorized by the President and Congress to do so through a program like the Naval Reactors program for nuclear propulsion. Conditions for current NRC reactor licenses are specified in 10 CFR 50.54. These conditions provide a basis for evaluating potential licensing issues for any microreactor design that intends to implement a high degree of autonomous control. Some of the license conditions that may be problematic for highly autonomous reactors relate to staffing, manipulation of controls, licensed operators, technical specifications (TSs), cybersecurity, and notifications.

Current regulations regarding licensed reactor operator staffing are based on existing large light-water reactors (LWRs) that rely primarily on active safety systems and operator actions to address plant transients and design basis accidents. 10 CFR 50.54(k) and (m) are very specific regarding control room staffing. The NuScale small modular reactor (SMR) design was developed to support justification for an exemption from this requirement because the passive safety systems, simplicity of operation, automation, reduced licensed operator workload, limited important human actions, and ample time to complete operator actions collectively indicate that licensed operator staffing levels would be different than that anticipated in 10 CFR 50.54(m). These attributes should also be associated with a reactor design with a high level of autonomous control.

In addition to the staffing requirements identified in 10 CFR 50.54, 10 CFR 50.47 establishes requirements for nuclear power plant emergency response plans. 10 CFR 50.47(b)(2) requires that adequate staffing be provided, but it does not specify a regulatory requirement for the number of licensed operators required to provide for on-shift accident response. NUREG-0654 provides evaluation criteria for determining what constitutes adequate staffing, and it provides guidance on staffing levels that the NRC has deemed acceptable. Staffing at a microreactor with a co-located facility may require smaller staffing levels and fewer security forces, but complete elimination of staffing will be unlikely.

Licensed operators must be fully aware of any manipulation of reactor controls, including apparatuses and mechanisms other than controls that may affect the reactivity or power level of the reactor, as discussed in 10 CFR 50.54(i) and (j). Operator knowledge and consent are key components of this regulation. Highly autonomous reactor designs must prove significant safety margins regarding reactivity insertions and power level changes.

From the time a reactor commences operation until the plant is decommissioned, regulations require that licensed operators be continuously present at the controls. Licensed operators continuously turn responsibility for the plant over, including official designation of the person responsible for the controls at any moment. This extends to bathroom and food breaks. An *operator* is defined in 10 CFR 55.4 as "any individual licensed under this part to manipulate a control of a facility." Likewise, a senior operator is defined as "any individual licensed under this part to manipulate the controls of a facility and to direct the licensed activities of licensed operators." It is conceivable that the reactor control room may not be co-

[4] R. J. Belles and M. D. Muhlheim, "Licensing Challenges Associated with Autonomous Control," ORNL/SPR-2018/1071 (December 2018).

located with the nuclear power plant due to implementation of highly autonomous controls in the design and remote siting. However, licensed operators are required under current regulations.

Various requirements in 10 CFR 50.54 reference operating in accordance with TSs. Therefore, highly autonomous reactor designs must consider TSs regarding design safety limits, limiting safety system settings, and limiting control settings as discussed in 10 CFR 50.36. A highly autonomous reactor design must operate the reactor according to TS guidelines, provide for appropriate equipment surveillance, and provide acceptable recordkeeping and other administrative controls. Onsite licensed and unlicensed operators currently provide for equipment surveillance and the associated recordkeeping.

Security, including cybersecurity, is a required condition of any license as directed in 10 CFR 50.54(p)(1) and as expanded in 10 CFR 73.54. Each licensee must provide high assurance that digital computer and communication systems and networks are adequately protected against physical and cyberattacks. Highly autonomous reactor designs will interface directly with safety-related and important-to-safety systems and functions. Therefore, cybersecurity will be an important consideration for any highly autonomous reactor design to demonstrate adequate protection of the health and safety of the public and the environment.

Therefore, from a regulatory perspective, a highly autonomous reactor must be designed so the following requirements can be met:

1. notifications are made automatically as required,
2. operating staff are apprised of notifications that must be made in a timely manner.

Highly autonomous microreactors will likely need to demonstrate a high degree of passive safety and a small source term. Such attributes will allow a minimal emergency plan, which could lead to reduced onsite staffing, including security, and will potentially allow a remotely located control room.

2. HISTORY OF ADVANCED CONTROLS AND AUTONOMY

The area of automatic feedback controls has a rich history that can be traced back to the 9th century. However, automation as we know it today began to become a reality with the industrial revolution, particularly with the emergence of the steam engine. *Autonomy*—i.e., operation without relying on human intervention—is in large part an advancement that appeared with the invention of computers and programmable devices that could perform fairly complex computations. This section presents some examples of advanced controls and autonomy from a wide range of applications. These applications provide insights into the requirements and the architecture for autonomous control in nuclear systems.

2.1 AUTONOMY IN ROBOTICS

A plethora of architectures has been developed for autonomous systems. Historically, the dominant view was that the control system could be divided into three functional elements: (1) the sensing system, (2) the planning system, and (3) the execution system. The sensing system, which is actually the data acquisition system, translates raw sensor data into a world model, which the planner uses to generate a plan based on predefined goals. Then the plan is used by the execution system to generate the prescribed actions. This basic architecture is called *sense-plan-act* (SPA) or *sense-plan-execute* (SPE).[5]

[5] N. J. Nilsson, "Principles of Artificial Intelligence," Palo Alto: Tioga (1980).

2.1.1 Subsumption

In the mid-1980s, Brooks introduced the subsumption architecture for autonomous robots[6]—the first known departure from SPA. The subsumption architecture was built in layers, with each layer giving the system a set of pre-wired behaviors. The higher levels were built upon the lower levels to create more complex behaviors. In a subsumption architecture, the system's behavior is the result of many interacting simple behaviors, with each layer operating 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 or output of that AFSM is activated. The inputs of AFSMs originate from sensors or from other AFSMs. The outputs of AFSMs are sent to the agents' actuators or to the inputs of other AFSMs. Each AFSM accepts a *suppression signal*, which overrides the normal input signal, and an *inhibition signal,* which causes output to be completely inhibited. These signals allow behaviors to override each other so that the system can produce coherent behavior.

2.1.2 T/R-III

A leading successful architecture that followed subsumption was T/R-III. Unlike subsumption, T/R-III embraces abstraction rather than rejecting it. In subsumption, higher level layers interface with lower levels by suppressing the results of the lower level computations and superseding their results, However, in T/R-III, higher level layers interface with lower-level layers. Autonomous robots with the T/R-III architecture were among the first robots capable of reliably performing a task that was more complex than simply moving from place to place. However, these robots had one serious drawback: the task they performed could not be changed without rewriting the control program.

2.1.3 Remote Agent

Remote Agent (RA) architecture was developed and tested as part of the Deep Space 1 mission. The RA architecture includes the *Mission Manager* (MM), the *Planner/Scheduler* (P/S), the *Smart Executive* (EXEC), and the *Mode Identification and Reconfiguration* (MIR) modules in a relatively flat structure. These modules are allowed to interact in a matrix composition.[7] The MM and the P/S modules perform a tightly coupled function that is possible because the MM maintains the mission profile that guides planning for the mission's 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, a control manager that executes the sequence of activities and reacts to failed responses. The EXEC module 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 can 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.

[6] R. A. Brooks, "A Robust Layered Control System for a Mobile Robot," *IEEE J. Robotics and Automation*, v. RA-2, No. 1 (1986).
[7] N. Muscettola et al., "On-Board Planning for New Millennium Deep Space One Autonomy," *Proc. IEEE Aerospace Conference*, Vol. 1, pp. 303–318, IEEE, Snowmass, Colorado (February 1997).

2.1.4 CLARAty

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*.[8] The decision layer interacts with a separate functional layer at all levels of system granularity. The functional layer is an object-oriented software hierarchy that provides basic capabilities of system operation, resource prediction, state estimation, and status reporting. The decision layer uses the capabilities of the functional layer to achieve goals by expanding, ordering, initiating, and terminating activities. The CLARAty architecture implements both declarative and procedural planning methods.

The Mars Technology Program funded development of autonomous control architecture to support the *Mars Exploration Rover* (MER) mission. The CLARAty software environment supports autonomy for the Rover's *Spirit* and *Opportunity*. The CLARAty architecture provides an upper decision layer for artificial intelligence (AI) software and a lower functional layer for controls implementations. In effect, the CLARAty architecture collapses the planner and executive levels, which are characterized by high levels of intelligence, into the decision layer.

2.2 SPACE SHUTTLE

The Space Shuttle Main Engine (SSME) control system was upgraded to adopt advanced performance and reliability in military jet engine controls. The SSME works through a hierarchy of various control and diagnostic functions, including life-extending control, real-time identification, and sensor/actuator fault tolerance.[9] AI, if-then logic, rule functions based on requirements, and onboard real-time models are all used for the engine-level coordinator function. The intelligent control system increases the autonomy of the engine controls by becoming self-diagnostic, self-prognostic, self-optimizing, and mission adaptable. The intelligent control hierarchy structure consists of lower levels operating in a real-time manner with the subsystems. The structure consists of algorithmic tasks with less intelligence and upper levels operating on a longer real-time scale with more intelligence. In other words, the lower level provides the closed-loop control and basic diagnostics. The upper level evaluates the ability to carry out the mission. The upper level communicates status and health to the propulsion level control.

The life-extending control function provides the desired steady state and transient performance with reductions in component fatigue due to mechanical, thermal, and other effects.[10] This is primarily accomplished by adjusting the engine acceleration schedule and control, which accelerates the fan and core to provide the desired thrust within the required time. The adjustment of these schedules delivers a balanced response between transient performance and minimal component damage. Another aspect of life-extending control is *active clearance control*. As the engine components degrade, the control can track the degradation and adjust the control action to provide a balance between engine performance and long-term reliability.

2.3 UNMANNED AERIAL VEHICLES

As the tasks and roles of unmanned aerial vehicles (UAVs) increase, so do the requirements to increase their level of autonomy and intelligence. UAVs are employed for intelligence gathering, surveillance, reconnaissance missions, fighting wildfires, traffic reports, and border security. UAVs are often tasked

[8] R. Volpe, I. Nesnas, T. Estlin, D. Mutz, R. Petras, and H. Das, "The CLARAty Architecture for Robotic Autonomy," *Proc. IEEE Aerospace Conference*, Vol. 1, 121–132, Big Sky, MT (March 10–17 2001).
[9] J. S. Litt, et al., "A Survey of Intelligent Control and Health Management Technologies for Aircraft Propulsion Systems", NASA/TM-2005-213622, ARL-TR-3413 (May 2005).
[10] J. S. Litt et al., "A Survey of Intelligent Control and Health Management Technologies for Aircraft Propulsion Systems," NASA/TM—2005-213622, ARL–TR–3413, May 2005.

with detecting and tracking a target of interest in a dynamic and uncertain environment, for example. This operation typically requires processing large quantities of sensory and communicated information. Autonomous functions and capabilities for UAVs are typically categorized as sensor fusion, communications, path planning, task allocation and scheduling, and cooperation with other resources.

The UAV onboard decision-making subsystems consist of sensory processing, path planning, and autopilot. Sensory processing uses various sensory inputs to determine state estimates of desired targets or parameters of interest. The path planning uses information such as global positioning system (GPS) locations, communication data about other UAVs, and the state estimate of the desired target to determine a desired path.[11] The desired path is then executed through the auto pilot control and the low-level vehicle control system.

Target estimation and tracking are performed using probability maps, Kalman filtering, and rule set. Sensor processing is performed using Kalman or particle filtering techniques.[12] The autopilot interfaces between the higher-level decision-making capabilities and the air vehicle. The autopilot uses models of the vehicle's dynamics, state estimates, and measurements to properly follow the desired flight path.

2.4 HIGHLY AUTONOMOUS DRIVING

Highly autonomous driving is emerging as one of the most controversial technological innovations, with huge socioeconomical implications. While specifics of implementations may vary from one vendor to another, the behavior of drivers is often modeled by a two-layered agent architecture: the tactical layer and the strategic layer. The *tactical layer* orients to short time-scale driving, while the *strategic layer* addresses complex problems such as route choice and decision-making. Two particularly difficult tasks in driving are recognizing when it is safe to change lanes or when it is safe to make a left turn. Some of the most advanced and exciting applications in automated decision-making appear in autonomous driving, as shown in recent efforts by several major universities and corporations, including Stanford University, Google, and BMW Group.

2.4.1 Stanford University

Stanley and *Junior* are autonomous cars created by Stanford University's Stanford Racing Team in cooperation with the Volkswagen Electronics Research Laboratory (ERL). Both vehicles are equipped with custom-built systems to enable direct actuation of throttle, brakes, transmission, and steering. Vehicle data are accessed by a computer control system through the vehicle's controller area network (CAN) bus interface.

The autonomous control system is comprised of three top-level functional elements: (1) perception, (2) planning, and (3) control. The processing unit used in Stanley consists of approximately thirty modules executed in parallel. Both Stanley and Junior both have modular software architectures. The modules run asynchronously and transmit data from sensors to actuators in a pipeline fashion: first-in, first-out (FIFO). The modular architecture reduces system reaction time.

The *sensor interface layer* comprises a number of software modules concerned with receiving and time-stamping all sensor data. The *perception layer* maps sensor data into internal modules. The primary module in this layer is the unscented Kalman filter vehicle state estimator, which determines the vehicle's coordinates, orientation, and velocities. The *control layer* is responsible for regulating the steering,

[11] J. P. How, C. Fraser, C., K. C. Kulling, L. F. Bertuccelli, O. Toupet, L. Brunet, A. Bachrach, and N. Roy, "Increasing Autonomy of UAVs, Decentralized CSAT Mission Management Algorithm," *IEEE Robotics & Automation Magazine*, June 2009.
[12] M. Lundell, J. Tang, J., and K. Nygard, "Fuzzy Petri Net for UAV Decision-Making," *Proc. 2005 International Symposium on Collaborative Technologies and Systems*, 2005.

throttle, and brake response of the vehicle. A key module is the path planner, which sets the trajectory of the vehicle in steering- and velocity-space. This trajectory is passed to two closed-loop trajectory tracking controllers, one for the steering control, and one for the brake and throttle control. The control layer also features a top-level control module, which is implemented as a simple finite state machine.

Estimation of the vehicle's state is essential to precision driving. Inaccuracies in pose estimation can cause the vehicle to drive outside the corridor or to build terrain maps that do not reflect the state of the robot's environment, leading to poor driving decisions. Stanley's *vehicle state* comprises a total of 15 variables.

Driving decisions are made using path-planning methods which generate multiple local trajectory options. These options are then weighed against a number of criteria, such as minimization of the risk of collision, as well as favoring the road centers over paths closer to the periphery.

For global path planning, a dynamic programming algorithm called A* is employed to search for shortest path, which minimizes the expected drive time to the target location. It typically takes the global search about one second to execute and generate an optimal solution. However, unexpected changes in the terrain (for Stanley) or traffic complications such as lane changes (for Junior) require local but discrete refinements to the global solution. Furthermore, for *unstructured navigation* such as driving in parking lots or for parking, Junior uses a modified version of the A* algorithm, which searches for shortest path relative to the vehicle's map using *search trees*.

Junior employs a decision module to minimize the risk of getting stuck in unpredictable environments, such as urban driving conditions. The decision module is implemented as a finite state machine. While the path planner, which can be considered as the global optimizer, works best under normal driving conditions, the finite state machine accounts for driving surprises. Following an impasse, the finite state machine gradually transitions to increasingly unconstrained driving.

2.4.2 Google Self-Driving Car

Google's *self-driving car* technology—occasionally referred to as the *Google driverless car*—is a demonstration concept car for autonomous driving. Google's autonomous vehicle is an improvement on Stanley and Junior. Originally implemented on a Toyota Prius, Google's concept vehicle includes a light detection and ranging (LIDAR) system which uses a 64-beam laser. The laser allows the vehicle to generate a detailed 3D map of the environments. The processor then combines the imagery with high-resolution maps to enable self-driving while avoiding obstacles and following traffic laws.

The vehicle also includes other sensors, including four radars mounted on the front and rear bumpers, allowing the car to detect obstacles and other vehicles in close proximity to deal with fast traffic on freeways; a camera positioned near the rear-view mirror to detect traffic lights; a GPS; an accelerometer for inertial measurements; and a wheel encoder to determine the vehicle's location and movements.

Since details on Google's technology are not publicly available, a review of Stanley's autonomous control technology will be used to gain insight into the specifics. Google's fleet of robotic cars is reported to have driven over 300,000 km at this writing, including driving in city traffic, busy highways, and mountainous roads, with only occasional human intervention.

2.4.3 BMW Highly Autonomous Driving

The BMW Group Research and Technology is developing highly automated assistance and active safety systems for future car generations.[13] An example is the *emergency stop assistant*, which takes over vehicle control, safely steers the vehicle to the side of the road, and stops if the driver suffers a health irregularity or possibly a heart attack.

Highly autonomous driving (HAD) technology is advancing current vehicular automation by providing additional driving assistance. Information concerning the host vehicle's environment (road, lanes, and objects) is provided online through the vehicle's sensors and a high-precision digital map. The raw sensor data and map data are processed within the subsequent *Perception* unit. The *Object Tracking* module fuses the data of multiple sensors and generates a global object list which includes the objects' attributes.

Based on traffic conditions, decisions should be made to identify suitable driving maneuvers for the vehicle. The BMW approach uses a hierarchical, hybrid decision-making process, which has a limited number of discrete system states that classify various driving maneuvers. This approach combines a finite state machine for *deterministic* aspects and decision trees to account for the *probabilistic* aspects of decision making.

A *lane change* request is executed if the maneuver is desired and feasible. If a lane change is desired but is not feasible, then the *lane change gap approach* strategy is applied. This approach helps avoid some of the potential problems with probabilistic approaches with direct influence on driving maneuvers, which were shown to lead to nondeterministic behavior, or sometimes infringement of traffic rules.[14]

This combined approach increases the robustness of the decision-making process by adding a feasibility analysis of driving requests. While the probabilistic approach accounts for environmental and systematic uncertainties and generates a desired driving behavior, the rule-based deterministic approach considers the worst-case conditions and eliminates or avoids unfeasible driving requests.

The probabilistic aspect of the decision-making process is implemented using a modified version of *utility theory*, which evaluates the utility of each lane—that is, the suitability for the vehicle—and generates lane change requests. This approach allows for incorporating uncertainties associated with sensor data, as well as those resulting from sensor fusion and state estimation.

The utility function consists of multiple factors that evaluate the utility of a lane based on various comfort and safety criteria. Weights for the utility function are determined based on a number of factors, including but not limited to general traffic characteristics such as the average longitudinal gap size between objects and the average velocity on a lane, or the specific velocities and distances of single objects.

2.5 NUCLEAR POWER PLANTS

The degree of nuclear power plant automation varies depending on the vendor and the facility generation. Almost exclusively, all US nuclear power plants are baseload generators that eliminate the need for power maneuvering. Moreover, existing feedback control systems can handle setpoint tracking with excellent stability and reasonable performance. Therefore, the need to move toward autonomy or even more automation has not been a priority for the industry. However, with the changing economic landscape, advanced reactors, and smaller sized reactors comprised of multiple units, automation and even some

[13] M. Ardelt, C. Coester, and N. Kaempchen, "Highly Automated Driving on Freeways in Real Traffic Using a Probabilistic Framework," *IEEE Transactions on Intelligent Transportation Systems*, 13(4), pp. 1576–1585 (2012).
[14] M. Ardelt, P. Waldmann, N. Kämpchen, and F. Homm, "Strategic decision-making process in advanced driver assistance systems," *Proc. IFAC Symp. AAC*, Munich, Germany (2010).

degree of autonomy are beginning to gain attention—primarily to enable significant staffing reduction and to allow for more informed and strategic maintenance planning. Additionally, interest in more flexible operations, such as load following, in response to diversification of energy sources to include solar and wind with intermittent output, further underlines the attention on autonomy.

There are a number of notable examples within the existing plants. The first DOE R&D in autonomy can be traced back to the Advanced Liquid Metal Reactor (ALMR) program.

2.5.1 Existing Systems

A number of advanced control systems are in use at nuclear power plants. For example, the basic requirement for an integrated control system (ICS) at a B&W-designed plant is the matching of generated electrical output with demanded output.[15] The ICS accomplishes this requirement through four subsystems:

1. The unit load demand functions as a megawatt electric setpoint generator for the ICS and can be used to adjust reactor power between 15–100%.
2. The integrated master 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.
3. The feedwater demand converts the megawatt demand signal to a feedwater demand in the integrated master and controls the amount of feedwater supplied to the steam generators.
4. The reactor demand moves the control rods in response to the megawatt demand signal, and it also maintains the average reactor coolant system temperature at a given setpoint.

2.5.2 Research and Development Activities on Autonomous Control

There is an architectural approach for nearly autonomous control systems that has been applied through simulation for nuclear power applications. As part of a research effort 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.[16] 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 illustrated in Figure 1 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.

[15] US Nuclear Regulatory Commission, "Pressurized Water Reactor B&W Technology Cross- training Course R-326C, Manual Chapter 9.0, Integrated Control System," NRC ADAMS Accession No: ML11221A266 (2011).
[16] P. J. Otaduy, C. R. Brittain, L. A. Rovere, and 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).

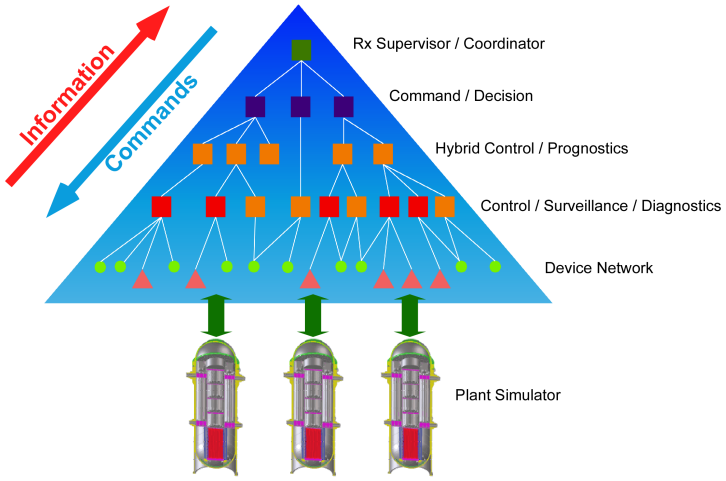


Figure 1. Supervisory control architecture proposed for multi-module nuclear power plants.

2.6 DEGREE 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 into these control systems to improve system resilience and increase overall system availability. Table 1 suggests a scale of *degrees of automation* as proposed by Sheridan.[17]

As the level of autonomy increases, so do the likelihood and potential consequences of machine error, while precluding human intervention. Therefore, the degree of autonomy is a design decision that must be determined as a trade-off between staffing reduction, operational flexibility, system complexity, and potential safety and reliability implications.

Table 1. Degree of automation[17]

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 the computer decides to;
10	The computer decides everything and acts autonomously, ignoring the operator

[17] T. B. Sheridan, *Telerobotics, automation, and human supervisory control*, The MIT Press, Cambridge, Massachusetts (1992).

2.7 ARCHITECTURE FOR AUTONOMOUS CONTROL

Architecture is a conceptual model that defines the rules between SSCs or *entities*, to include the relationships, dynamics, and interactions in a system. An architecture is a formal description and representation organized to support reasoning about structures of the system, components, interfaces, relationships, and the interactions between them [18,19].

Architecture for autonomous control provides a method to describe complex systems in terms of abstract entities. It can be used to represent multiple components in a system that share common attributes, defining the elements of a system and imposing high-level rules to describe how the elements connect and interact with each other to fulfill the mission.

An abstraction of the flow of information for a generic nuclear power plant is presented in Figure 2. As can be seen, an operator's role is to identify and execute control actions. The operator must 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 they may also develop high-level commands.

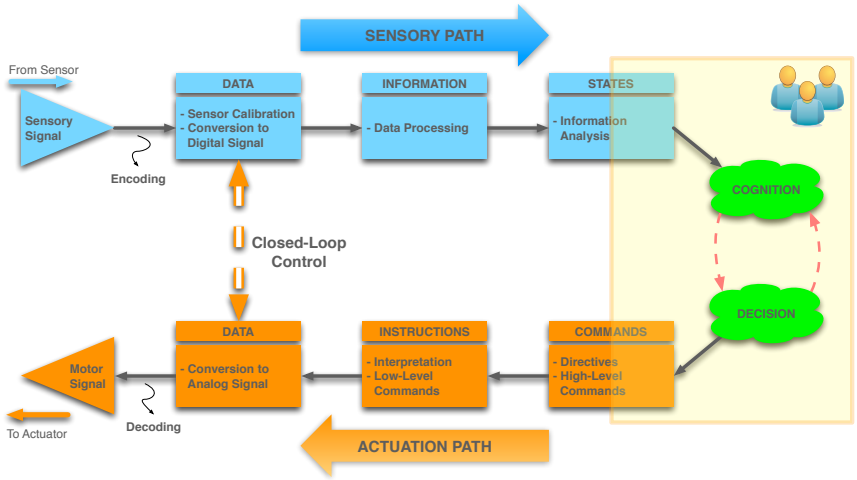


Figure 2. Flow of information in a sense-command-execute loop.

2.7.1 The Rationale Behind Three-Layer Architectures

These observations lead to the following questions:

- Why do so many independently designed architectures have similar structures?
- Are three layers necessary or sufficient, or is the number three a coincidence?

It has been shown that the three distinct layers of functionality are essentially the result of methods to manage the *internal state* information.[20] *Decision-making* and *planning* require that certain data be stored (i.e., the internal state) during complex 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 obvious

[18] Standard ISO/IEC/IEEE 42010:2011, Systems and software engineering – Architecture description
[19] Hannu Jaakkola and Bernhard Thalheim. (2011) "Architecture-driven modelling methodologies." In: *Proceedings of the 2011 conference on Information Modelling and Knowledge Bases XXII*. Anneli Heimbürger et al. (eds). IOS Press. p. 98
[20] E. Gat, "On Three-Layer Architectures," in Artificial Intelligence and Mobile Robots, D. Kortenkamp et al., eds., AAAI Press.

solution is to eliminate the use of internal states. However, this requires fast sampling, as well as high bandwidth and computational power. Technological advances eliminate the first two problems, but computational power may still be an issue for *nondeterministic polynomial-time hard* (i.e., *NP-hard*) problems such as global optimization algorithms that may require an extensive search for minima. From the internal state perspective, three-layer architectures organize algorithms according to the following principles:

1. a functional layer containing no internal state,
2. a coordination layer containing memory about the past, and
3. an organization layer containing memory about the future.

The *functional layer* consists of one or more threads of computation that implement a series of feedback control loops. These are conventional loop control algorithms, which map sensors directly onto actuators with little or no internal state. The *coordination layer* is an intermediate level that contains algorithms for governing routine sequences of activity; these sequences rely extensively on internal state, but they do not require time-consuming searches. The *organization layer* sits at the top of the computational hierarchy and is responsible for performing the more time-consuming calculations.

The three-layer architecture essentially provides a graded abstraction at each 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 descend through the hierarchy. Higher levels are concerned with slower aspects of the system's behavior, and they are responsible for planning with a longer time horizon.

2.8 DECISION MAKING AS A RATIONAL PROCESS

Decision-making is one of the basic cognitive processes of human behaviors by which a preferred option or a course of actions is chosen from a set of alternatives based on certain criteria. Decision theories are widely applied to various disciplines, including cognitive science, computer science, management science, economics, sociology, psychology, political science, statistics, engineering, and business.

Mathematically, decision-making is a problem-solving activity to identify and analyze the available courses of action and to determine the most appropriate option given the set of conditions and constraints. The solution space can differ vastly, depending on the nature of the problem being solved.

As engineering systems and the processes have become increasingly more complex, with significantly higher degrees of interconnectedness, designing automation systems to address a wide range of operating conditions and equipment availability has become a daunting task. Logic tables that are usually used to address a limited set of scenarios under nominal conditions are not comprehensive enough to cover all possible actions as a function of various system conditions. Therefore, capabilities are needed to (1) diagnose a situation, (2) identify viable course of actions, and (3) determine the best, optimal or at least an acceptable action or a sequence of actions to transition to a safe state. This process is called *decision-making*.

The sections below provide a brief summary of the analytical methods and tools used for decision-making. A more detailed discussion on decision-making can be found in Cetiner's "Development of an Automated Decision-Making Tool for Supervisory Control System."[21]

[21] S. M. Cetiner, et al., "Development of an Automated Decision-Making Tool for Supervisory Control System," ORNL/TM-2014/363, Oak Ridge National Laboratory (September 2014).

2.8.1 Statistical Decision Theory

Statistical decision theory is concerned with making decisions based on statistical knowledge, which sheds light on some of the uncertainties involved in the decision problem. The field of classical statistics is directed toward using sample information arising from statistical investigation to make inferences about the use of the data. In contrast, *decision theory* attempts to combine the sample information with other relevant information, with the intention of making the best decision.

In addition to sample information, two other types of non-sample information are typically relevant. The first is the *knowledge of possible consequences of decisions*. Often this knowledge can be quantified by determining the loss that would be incurred for each possible decision and for various possible values of uncertainties. The incorporation of a loss function into statistical analysis was first studied extensively by Wald.[22]

The second source of non-sample information that is useful to consider is called *prior information*. This is information about uncertainty arising from sources other than statistical investigation. Generally, prior information comes from past experience about similar situations involving similar uncertainties.

2.8.2 Bayesian Decision Theory

The Bayesian approach is one of the most commonly referenced mathematical methods used in decision-making processes in a wide range of applications. In Bayesian decision theory, the choice function is called a *decision rule*. A loss function is adopted to evaluate the consequences of an action. Using the loss function to determine possible risks, a choice function is derived for decision-making.

A generic Bayesian decision process can be divided into two phases: the *inference phase* and the *decision phase*. In the inference phase, posterior probabilities are obtained using the prior information associated with the random processes used in the decision-making process. In the decision phase, alternative decisions are identified, and an optimal decision is determined based on the construct of the loss function.

2.8.3 Utility Theory

Utility theory was developed by economists to explain and predict human decision-making under risk and uncertainty. The fundamental assumption underlying utility theory is that the decision maker always chooses the alternative for which the expected value of the utility is maximized. Built into this assumption is a further supposition that a code of rationality is accepted and utilized by human decision-makers, thus making it possible to construct a mathematical representation that allows prediction of human behavior.

The basic approach of utility theory can become a foundational building block for a decision-making system intended for real-time autonomous control. Given a collection of seemingly viable alternative solutions, implementation risks determined for each alternative can be compared to find a minimum risk solution. Independent loss and gain (utility) functions as related to plant operating procedures or other decision strategies can be formulated and represented as nonlinear relationships.

[22] A. Wald, "Basic Ideas of a General Theory of Statistical Decision Rules," *Proc. of the International Congress of Mathematicians*, 1, pp. 308–325 (1950).

2.8.4 Markov Decision Processes

Markov Decision Processes (MDPs) provide a mathematical framework for modeling decision-making in situations where outcomes are partly random and partly under the control of a decision maker.[23] MDPs have been used successfully in a wide range of autonomous control problems[24,25] and typically solve an optimization problem using *dynamic programming* (DP) for selecting the *right* decision. A partially observable Markov decision process (POMDP) is a generalization of an MDP.[26] A POMDP models a decision process in which it is assumed that the system dynamics are represented by an MDP, but not all states are observable. Instead, the measurements received by the model are incomplete and are usually noisy predictions. Therefore, the model must estimate a posterior distribution over a possible state space.[27] POMDPs compute a value function, which is similar to a cost function in optimal control, over a *belief* space. A belief is a function of an entire probability distribution. An exact solution to a POMDP yields the optimal action for each possible belief over the state space, which maximizes the value function. However, this maximization procedure requires an iterative algorithm that is far from practical. For any reasonable number of states, sensors, and actuators, the complexity of the value function is prohibitive. Therefore, significant research has been conducted on the efficiency and optimality of solutions, with differential dynamic programming (DDP) being a promising DP-based solution method for large-scale problems, as it only optimizes over the unconstrained control space.[28] DDP is an optimal control algorithm of the trajectory optimization class. It is a powerful method because (1) it explicitly exploits system dynamics, (2) its solution has certain feedback nature, (3) it avoids the curse of dimensionality of DP and requires no discretization of control/state variables, and (4) it is efficient for unconstrained dynamic optimization.

The *Lagrange-multiplier-based DDP method*[29] was developed to tackle a wide range of dynamic optimization problems with nonlinear constraints.[30] This approach first relaxes all constraints by using the Lagrange-multiplier method. For a given set of multipliers, there is an unconstrained dynamic optimization problem to which DDP applies effectively. The optimal solution is obtained by iteratively updating the Lagrange multipliers and solving the corresponding dynamic optimization.[31] Other emerging methods which have gained attention for efficiency and robustness include *sequential quadratic programming* (SQP), *generalized reduced gradient* (GRG), *trust-region* and *interior point* methods.
An important element of reasoning is to estimate the ranking of expected net benefits of alternative actions affecting SSCs of interest. This evaluation rests upon the estimated utility or the expected net benefits, including uncertainties, of alternative actions. These alternatives can be evaluated using state conditional probability estimates obtained from Bayesian probability updating or from MDP simulations. This type of evaluation requires knowledge of the costs and benefits, as well as the decision-maker's appreciation of available alternative actions, weighting of these variables in terms of the likelihoods of alternative future system SSC states, and associated expected evolution timescales.

To incorporate the system dynamics into the decision-making process, the utility variables must be selected such that the projected physical behavior of the system can be factored in. One such approach

---

[23] M. L. Puterman, "Markov Decision Processes: Discrete Stochastic Programming," Wiley-Interscience, New Jersey (2005).
[24] S. Thrun, "Stanley: The Robot than Won the DARPA Grand Challenge," *J. Field Robotics* **23**(9), 661–692 (2006).
[25] S. Brechtel, T. Gindele, and R. Dillmann, "Probabilistic decision-making under uncertainty for autonomous driving using continuous POMDPs," in *17th IEEE International Conference on Intelligent Transportation Systems*, pp. 392–399 (2014).
[26] K. J. Åström, "Optimal control of Markov process with incomplete state information," *J. Math. Anal. App.* **10**, 174–205 (1965).
[27] S. Thrun, W. Burgard, and D. Fox, "Probabilistic Robotics," The MIT Press, Cambridge, Massachusetts (2005).
[28] D. P. Bertsekas, "Constrained Optimization and Lagrange Multiplier Methods," Academic Press (1982).
[29] G. Lantoine and R. P. Russell, "A Hybrid Differential Dynamic Programming Algorithm for Constrained Optimal Control Problems. Part 1: Theory," *J Optim Theory Appl* (2012) 154:382–417.
[30] D. G. Luenberger, "Linear and Nonlinear Programming," Addison-Wesley Publishing Co. (1984).
[31] S.-C. Chang, C.-H. Chen, I.-K. Fong, P. B. and Luh, "Hydroelectric Generation Scheduling with an Effective Differential Dynamic Programming Algorithm," *IEEE Transactions on Power Systems*, 5 (3) (August 1990).

uses utility attributes based on key process variables that have safety implications, such as trip setpoints. The utility values are then calculated based on the proximity of these critical variables to trip setpoints.[32]

2.8.5 Discrete Event Systems

Many manmade devices and systems and some natural systems demonstrate only discrete values or outcomes. Manmade systems are governed by operational rules designed by humans. For example, manmade systems are often considered to be either on or off, enabled or disabled, running or stopped. These types of systems are best described as discrete event systems (DESs). They are not easily analyzed, nor are they designed using conventional mathematics and engineering with time-driven methods represented by differential equations. Examples include transportation traffic systems, computer systems such as interrupts, communication systems, manufacturing processes, games, and queuing systems. Opening and closing of valves or commencing a pump startup process are examples of discrete event processes in a nuclear power plant. These processes are typically tied to operating procedures, and their controls are handled by plant operators.

DESs satisfy the properties (1) that state-space is a discrete set, and (2) the state-transition mechanism is *event-driven*. Time in such systems is not the appropriate independent variable. Conventional differential equation approaches such as modern control theory do not apply to DESs.[33] They are described as:

> *A class of dynamic systems characterized as synchronous or asynchronous occurrences of various discrete-valued events. Values are described by discrete values and transitions only occur at discrete points in time. Events are considered to occur instantaneously with some transition of one discrete value to another discrete value. These may be considered as time-driven or synchronous systems or event-drive or asynchronous systems.*

DESs are typically modeled using an *automata* approach or a *petri net* approach. These approaches use a state-transition structure to describe the possible events in each state of the system. These two approaches differ in how they represent state information. An automaton is a device capable of representing a language according to well-defined rules and is commonly represented using a state-transition diagram with a defined set of states, initial states, events, and state-transition functions.

The choice of one of the three levels of abstraction (languages, timed languages, and stochastic timed languages) is made based on the system and the objectives of the analysis. If the analysis focused on the logical behavior as the precise ordering of events or what states are valid or invalid, etc., then the simple language approach is appropriate. In control system applications, a set of paths may need to be determined to achieve a desired state or set of stats. The language approach can be used to predetermine the desired set of paths in the logical behavior to achieve such desired states.

In some applications, the timed language approach can be useful to gain an understanding of the timing of events, event transitions, and event paths. This approach can answer questions such as "*How soon can a particular state are reached given the current state?*" or "*Given a particular state, how soon can an undesirable state be reached?*" The timed automata approach requires specific logical and timing information from a timed language description to answer questions about response time or throughput time. In other applications, the stochastic behavior must be included using probabilistic models in the stochastic timed languages abstraction. The language-based approach offers many benefits for understanding DESs.

---

[32] S. M. Cetiner et al., "Development of a First-of-a-Kind Deterministic Decision-Making Tool for Supervisory Control System," ORNL/TM-2015/373, Oak Ridge National Laboratory (July 2015).
[33] C. G. Cassandras, S. Lafortune, *Introduction to Discrete Event Systems* (Second Edition), Springer (2008).

Operations can be performed on these language sets using typical set operations such as union, intersection, difference, and complement. Other operations include concatenation, pre-fix closure, Kleene closure, and post-language. Projection operations are also performed on language sets.

A state transition automaton with internal states and outputs is called a *Moore automaton* or *Moore machine*. A state transition automaton with internal states, inputs, and outputs is called a *Mealy automaton* or *Mealy machine*. These automatons, which are well described in the literature, can be represented as an event set, E, and a state set, X.

An automaton that reaches a state which will not permit any further events to execute is called a *deadlock condition*. This condition is also describing as a *blocked condition* because the system will enter the deadlock state without completing the task at hand. If a system contains a set of states with a local sequence or cycle but does not have a transition to exit the local sequence, then that situation is described as a *livelock condition*. In a livelock condition, the system is not deadlocked, but it is cycling between states and cannot exit the particular cycle. These potential locked conditions lead to the topic of safety properties, which deal with the subject of reachability of undesirable states and the means to avoid blocked or livelock conditions. This process is followed during the finite state machine design.

An automaton can also include nondeterministic behavior. A nondeterministic automaton may demonstrate that, under some conditions, the state transition may have multiple outcomes. The primary source of nondeterminism in a physical DES is limited sensory information, which will result in unobservable events that drive varying state transition outcomes.

Petri nets offer an alternative modeling method for discrete event systems. A Petri net treats manipulation of events according to specific rules. A finite state machine can always be represented as a Petri net system and vice versa. A Petri net system is defined by its graph or structure, the initial state, the set of marked states, and a state transition function, as illustrated in Figure 3. The graph contains states, transitions, and relationships to describe the system behavior. The state transition mechanism in Petri nets is provided when a transition condition is enabled, and it results in a change of state.[34]

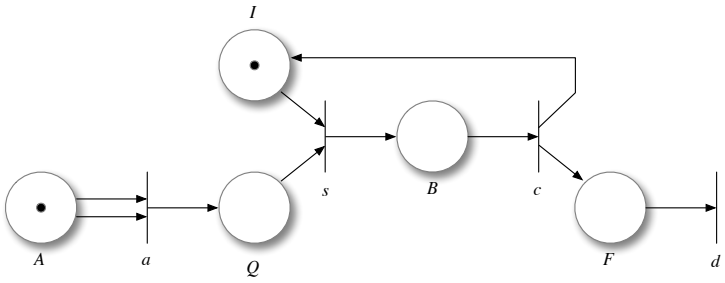


Figure 3. An example Petri net of a queuing system showing state transitions [adapted from Ref. 33].

2.8.6 Discussion on Appropriate Methods and Tools for TCR Autonomous Control

As discussed in Section 2.1 above, all successful implementations of autonomous controls address both the probabilistic and deterministic aspects of decision-making. Simply put, the probabilistic model captures the uncertainties associated with sensors as well as uncertainties that arise from modeling assumptions used in inferences. Examples include state observers such as Kalman filters. A deterministic model, on the other hand, imposes hard rules to assure that critical steps in a procedure are followed.

[34] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*, Springer (2010).

While search based algorithms such as those that rely on Bellman's *principle of optimality* provide a more realistic situational analysis, and hence awareness, implementation of these algorithms in industrial problems poses a risk for the aggressive schedule of the TCR program. Decision-making and supervisory control models based on discrete event systems—either finite state automata or Petri nets—have an established industrial track record, with applications ranging from robotics to self-driving cars. Based on this observation, it can be concluded that a supervisory control approach based on discrete event models offers the best approach for implementation of the TCR autonomous control system.

3. FRAMEWORK FOR TCR AUTONOMOUS CONTROL

The TCR autonomous control system shall comply with the following high-level requirements:

1. It shall be implemented as a non-safety–related system.
2. It shall meet all applicable rules and regulations regarding separation between and isolation of safety- and non-safety-related systems.
3. It shall not perform any safety-related function.
4. It shall not interfere with functionality of any safety system.
5. It shall not override operator commands.

These requirements will define the autonomous control system's domain of operation. Implementation as a non-safety–related system also minimizes licensing challenges. TCR operation will not require functionality of the autonomous control system, so it will be possible to start the reactor and bring it to full power level with the conventional instrumentation and controls (I&C) system using the control panels. The autonomous control functionality will provide a demonstration opportunity when enabled.

3.1 SCOPE OF AUTONOMY IN THE TCR

The fundamental assumption for the design of the autonomous control system is, if the system fails to act during a transient, then the safety system will independently initiate reactor scram and residual heat removal systems, bringing the plant to a shutdown condition. The scope of the TCR autonomous control system can be best described by the illustration in Figure 4.

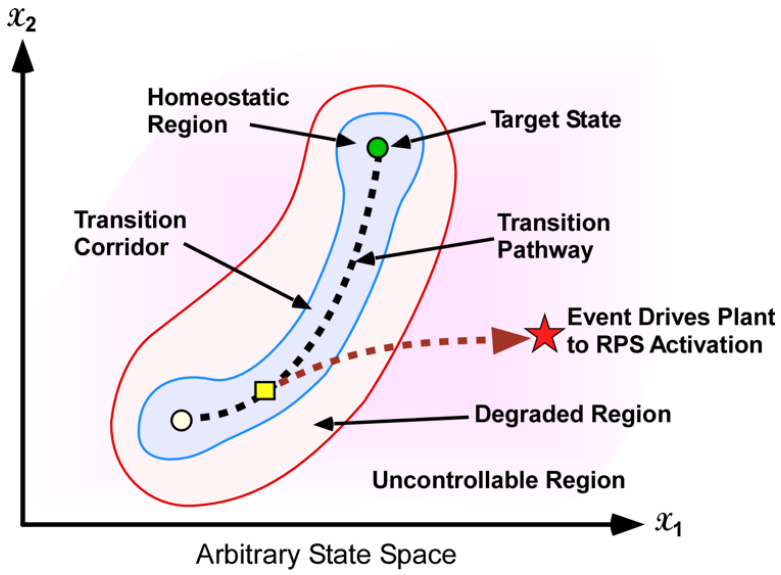


Figure 4. A conceptual state space formed by two arbitrary state variables.

Here the red line represents the *challenge surface*—a boundary delineated by the trip variables of the Reactor Protection System (RPS). Other definitions may also be possible. The autonomous control system is only allowed to function within the *controllable* domain. Once the RPS initiates for any violation of a safety variable, the interlocks will disable the autonomous control system functionality from interfering with the protection system executing its functions to completion.

3.2 SYSTEM-LEVEL FUNCTIONAL TAXONOMY

The objective of functional taxonomy is to enable consistent interface descriptions. The principal function of plant systems in a nuclear power plant is to transfer heat from the core to the power conversion system or to the ultimate heat sink. In this approach, it is proposed that the plant systems be divided into three tiers based on their functions in relation to the primary heat transport:

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

3.2.1 Tier-I Systems and Functions

Tier-I systems are those *directly* involved in the heat transport path from the reactor core to the ultimate heat sink. Tier-I functions are those performed by Tier-I systems. Systems in this tier provide direct interfaces for sensing the status of flow of heat, the integrity of critical SSCs, and the proper means for actuation to stabilize actions.

Traditionally, the systems in Tier I have a limited number of sensing and actuation interfaces. For instance, past high-temperature gas-cooled reactors (HTGRs) have employed only a limited number of in-core temperature measurements due to the high-temperature environment, while the traditional loop control signals for power level adjustments were generated by the power balance on the secondary side. Likewise, helium mass flow rate was not measured directly; instead, it was inferred based on the circulator shaft speed signal. Neutron flux measurements were also made external to the core—again because of high temperatures—using either fission chambers or compensated ion chambers. For controls, control rod drive mechanisms provided fast response to adjust power levels. These drive mechanisms were controlled by the error signal between the power setpoint and the measured power signal (flux) generated by the power range monitor (PRM). Past HTGRs such as Peach Bottom and Fort St. Vrain used variable-speed motors that drove a helium circulator turbomachinery. Proportional-integral (PI) control of a variable-speed motor provided a slow response to regulate reactor outlet temperature based on the error signal generated by the secondary-side outlet temperature, while the core inlet temperature was maintained by the control of coolant flow rate on the secondary side.

3.2.2 Tier-II Systems and Functions

Tier-II systems provide *direct* support functions for Tier-I systems. Tier-II functions are those performed by Tier-II systems. Tier-II systems and functions have particular significance for achieving the autonomous control functionality. Systems in this tier provide the necessary actuation interfaces for discrete-event–based control: activities performed by control room operators such as taking a pump off line while commencing a start-up sequence for a backup pump. They also provide additional sensor data for fault diagnostics to establish a holistic status of plant condition based on the condition of critical components.

The TCR system design is still evolving. Details of the sensing and actuation interfaces will be identified in the later phase of the I&C system design, while implementing the autonomous control system.

3.2.3 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. An example list of Tier-III systems based on previous HTGR designs is as follows:

1. plant electrical systems;
2. fire protection;
3. service water (of which there are several classes);
4. gas supply, to include argon, helium, nitrogen, compressed air and instrument air;
5. building environment, including heating, ventilation, and air conditioning (HVAC); and
6. hydraulic supply.

As indicated in the sections above, 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. As a matter of fact, the line between the two tiers is a trade-off between flexibility vs. cost, and system complexity. To move a system (or a subsystem or component) from Tier-III to Tier-II, the system of interest should be provided with additional sensing, as well as actuation means and interfaces, to perform the functions automatically.

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*. These events typically result in a reactor trip, and they affect the performance of front-line systems, including normal residual heat removal, passive residual heat removal, core makeup tank, and main and start-up feedwater. These initiators are identified by reviewing the plant design, support system, and abnormal operating procedures.

3.3 ALLOCATION OF FUNCTIONS

Autonomous control involves more than simple automation of routine functions. It also includes detection of conditions and events, determination of appropriate responses based on situational analysis, adaptation to unanticipated events or degraded/failed components, and reevaluation of operational goals.

As illustrated in Figure 5, the functions necessary for reliable plant operation are allocated between the human operator and the automation agents. Allocation of functions requires careful evaluation of work conditions and task loads, and it also requires a precise balance between reducing the workload while maintaining the operator's situational awareness. The functional allocation of tasks between the human operator and automation defines the boundaries of the autonomous control system and establishes the basis for its requirements.

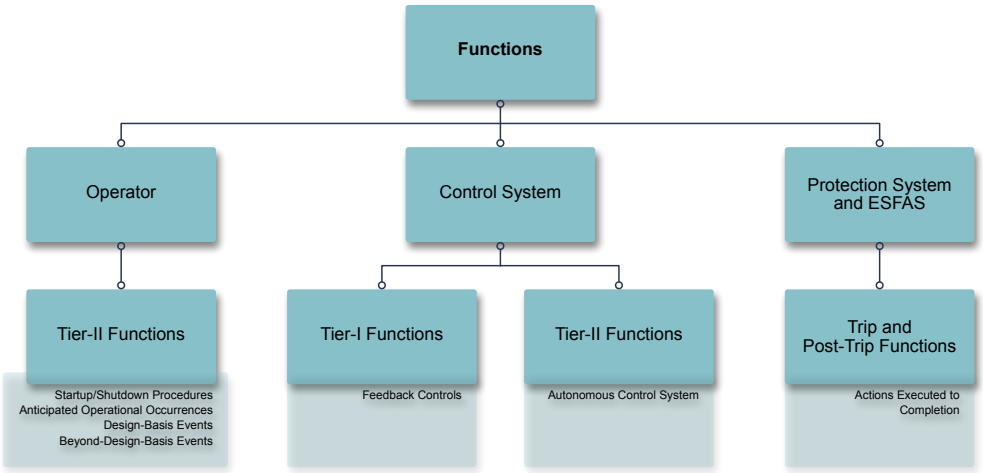


Figure 5. High-level allocation of functions between human operators, autonomous control system, and the protection system.

4. TCR CONTROL STRATEGY

This section describes progress made on high-level decisions for key elements and features of the TCR's I&C architecture. It also includes high-level requirements to enable the capabilities of the overall I&C system to deliver the required functions. I&C for advanced reactors is a mature technology. There is considerable national and international operational history with HTGRs. Many advanced reactors, including sodium-fast reactors (SFRs) and HTGRs, have operated with proven sensor technologies for extended period of times. For instance, Experimental Breeder Reactor II (EBR-II) went critical in 1965 and operated until its eventual shutdown in 1994. Similarly, the Fast Flux Test Facility (FFTF) achieved first criticality in 1980 and operated until 1992 as a national research facility. Fort St. Vrain (FSV) and Peach Bottom Unit 1 are examples of commercial HTGRs that operated in the United States.

The approach for the TCR I&C system design will minimize potential regulatory challenges for implementation of the I&C platform. This will be accomplished by relying on approved components and systems that have safety or safety-related functions—to the extent possible. For non-safety–related controls (i.e., the plant control system and other ancillary controls), more advanced control approaches can be adopted if they have sufficient industrial pedigree.

For the present application, autonomous operation focuses on moving the following human functions to algorithms:

- Step change in power level (increase or decrease) in response to an increase in demand
- Slow ramp between two steady state operation modes

4.1 AUTONOMOUS CONTROL ARCHITECTURE

TCR will adopt three-layer control architecture, as shown in Figure 4 and as discussed above in Section 2.1. The functions and high-level descriptions of individual layers are provided in subsequent sections.

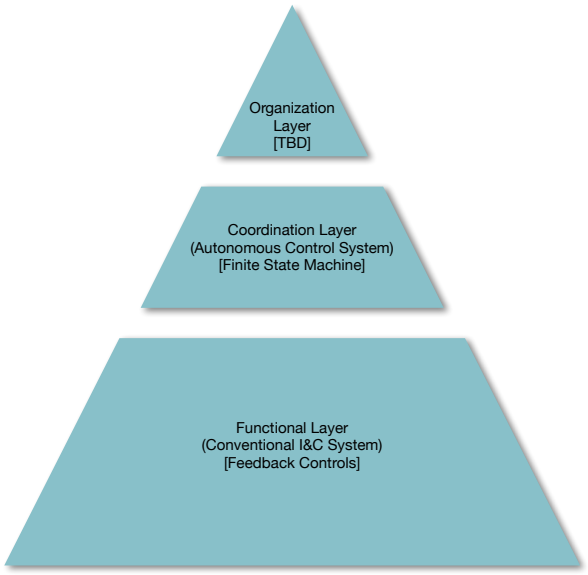


Figure 6. High-level architecture of TCR autonomous control system.

4.2 FUNCTIONAL LAYER—CONVENTIONAL I&C SYSTEM

The functional layer of the TCR autonomous control system architecture, as illustrated in Figure 4, includes sensors, actuators, and feedback control systems to perform the low-level control functions. This layer employs a conventional I&C system architecture designed to deliver a reasonable stability and a nominal setpoint tracking performance in the event of an anticipated operational occurrence (AOO). The TCR I&C system provides the hardware, software, and data communication infrastructure to enable sensing, monitoring, processing, actuation, and protective functions of the plant. Conceptually, the TCR I&C architecture is organized in two major divisions:

1. The conventional plant I&C system responsible for the protection and control functions; these are essential sensing and actuation functions that provide monitoring of key safety and performance variables and that generate reactor trip and plant control signals.
2. Extended monitoring to enable acquisition of data from key SSCs.

4.2.1 I&C System Architecture

A typical nuclear plant I&C system includes three major subsystems:

1. the Reactor Protection System (RPS),
2. the Plant Control System (PCS), and
3. the Data Communication System (DCS).

These subsystems fulfill distinct roles during the operational lifecycle of a nuclear reactor and all of its integrated systems. The RPS executes corrective actions to protect plant investment, and ultimately to protect public health and safety. The PCS continuously monitors key state variables and generates control actions. The DCS provides the communication infrastructure between sensors, processors, and actuators.

Consistent with the objective to minimize regulatory challenges, the RPS will be implemented on an endorsed analog platform or on endorsed off-the-shelf digital hardware platforms using either field-programmable gate arrays (FPGAs) or application-specific integrated circuits (ASICs). The PCS will be

implemented on industrial-grade FPGAs or programmable logic controllers (PLCs) with demonstrated pedigrees. Applicable codes, consensus industry standards, and regulatory guidance will be adopted commensurate with safety significance of the system. Established design practices will be followed in developing the I&C system architecture, such as proper isolation and separation of safety- and non-safety–related functions. All safety-related functions will be executed by Class-1E systems, platforms and components. Likewise, control system design will be minimized to avoid an undue risk that may arise from software qualification.

4.2.2 Reactor Protection System

The RPS includes the Reactor Trip System (RTS) to bring the reactor to a subcritical condition and maintain subcriticality. The RPS also provides additional post-trip functions to guarantee uninterrupted rejection of decay heat from the core. Evidently the RPS is designed to make sure that the nuclear safety limits are not violated, and as such, the plant is placed in a safe condition. Depending on the plant's needs and requirements, it may also provide isolation functions between systems to reduce the likelihood of proliferation of radiological species. The RPS is designated as a safety system.

The primary function of the RTS is to prevent the progression of design basis events (DBEs) or to limit the consequences of postulated initiating events by first initiating reactivity control procedures—called *reactor trip*—with the ultimate goal of meeting the off-site release limits defined in 10 CFR 100 to protect public health and safety. The RTS is classified as a safety-related system and is one of the principal safety-related defense measures.

The RTS actuation logic is created based on a methodical identification of initiating events (IEs) and postulated accidents (PAs), followed by an extensive analysis of DBEs. Protection system designs used in HTGRs are being used as a starting point, and the procedures are leveraged as guidance.

The preliminary list of safety-related measurements as the RPS trip variables include (1) reactor power-to-flow ratio, (2) helium flow rate, (3) core outlet temperature, (4) core inlet temperature, (5) ultimate heat sink status, and (6) power conversion system status—as shown in Table 2.

Table 2. Preliminary list of trip variables for the RPS actuation.

Trip variable	Physical measurement	System/component	Safety Indication
Reactor power-to-flow ratio	Neutron flux/He flow rate	Ex-vessel, circulator	Core overheating
Helium flow rate	Circulator $p, T, \Delta p$	Circulator	Loss of flow, depressurization
Core outlet temperature	Helium temperature	Intermediate heat exchanger	Overheating
Core inlet temperature	Helium temperature	Intermediate heat exchanger	Undercooling
Ultimate heat sink status	Trip signal	Air-dump heat exchanger	Availability, performance
Power conversion system status*	Trip signal	Balance of plant	Availability, load status

* Considered for completeness

As the TCR system design has not been finalized, it is premature to establish the power conversion system status signal as a trip variable at this stage. However, the first four variables presented here have been consistently used as trip variables in the history of HTGRs. As some or all of the heat will be rejected through air-dump heat exchangers, using the ultimate heat sink status as a trip variable makes sense.

4.2.3 Plant Control System

The PCS provides functions and capabilities to maintain operations of the reactor and other plant systems. These functions maintain the key operational variables for desired setpoints. If the plant is to deviate from those values, then the control system delivers incremental adjustments that guarantee stability to operations and that meet the desired performance requirements.

The function of the PCS is to regulate the plant variables consistent with irradiation needs while maintaining a balance between heat generation and heat removal so that plant temperatures remain within safe limits. This is achieved by sensing plant process variables and appropriately commanding actuators. The initial list of monitored variables for control purposes is shown in Table 3.

The core heat removal rate is managed by helium circulators (quantity yet unknown) using the error signal between the core average temperature setpoint and the measured average temperature as the tracking variable. The core inlet temperature is maintained by fine control of the air-dump heat exchanger circulator speed. By combining rod reactivity and flow rates, it is possible to keep the reactor coolant inlet and outlet temperatures essentially constant over the assigned load range.

Table 3. Preliminary list of control variables for the PCS tracking.

Control variable	Physical measurement	System/component	Control actuation
Reactor power	Neutron flux	Ex-vessel power range monitor (PRM) / wide range monitor (WRM)	Control rod or control drum
Core average temperature	Helium temperature	Intermediate heat exchanger	Primary helium circulator
Core inlet temperature	Helium temperature	Intermediate heat exchanger	Air-dump heat exchanger circulator

The TCR will use a feedback loop control approach such as PI control. Considering the simplicity of the plant, this approach should deliver good performance without undue complexity. Single-input-single-output (SISO) independent loop control will be considered as the baseline technology. More advanced control strategies can also be pursued, including multivariable state space feedback control. The advantage of state space feedback control is that (1) it allows coupling of multiple sensing and actuation signals enabling multiple-input multiple-output (MIMO) control approach, and (2) it also makes it possible to adopt control system design methods such as linear quadratic Gaussian (LQG) optimal control or robust control, delivering a more consistent performance over a wider operating range.

However, advantages of these advanced options are typically not as significant for simple systems such as the TCR. These methods are known to deliver better tracking performance and stability for systems with non-minimum phase behavior such as the shrink-swell dynamics in a steam generator drum or for systems that exhibit high nonlinearity.[35]

4.2.4 Instrumentation System

High-level sensing requirements for a nuclear reactor core resemble other process industries. The fundamental function of process measurements is to ensure that the heat rejected to the environment is equal to or closely tracks the heat generated by the source. The primary measurements include gross mass

[35] T. L. Wilson, W. K. Wagner, "Multivariable Control for the PRISM ALMR," Power Plant Dynamics, Control and Testing Symposium, Knoxville, TN (May 1989).

flow rate through the core and the mean temperature rise across the core. These measurements are used to confirm that the heat balance is satisfied, and the system integrity is not challenged.

For the present application, the sensed variables will include the quantities required to determine heat input from the core and the heat removal through the heat exchanger and heat dump systems. Other quantities may be included, depending on the desired functionality of the autonomous control system. Transmitters are included for conveying the measured quantity as part of the instrumentation system. It is particularly important to make the measurements in situ during plant operation. Most of the process parameters are always measured in situ in plants, but other quantities such as structural health and accumulated strain (elastic or plastic) are currently not measured in situ.

The specific sensors and instrumentation will consist of the trip variables defined as necessary for RPS actuation (see next subsection), process variables necessary (primary and secondary coolant flow rates, core inlet and outlet temperatures, air dump heat exchanger [HX] inlet and outlet temperatures, neutron flux) for confirming that the plant meets mission goals, and structural data to verify performance of the vessel internal components. Note that some of the plant's mission goal parameters are also important as trip variables.

4.3 COORDINATION LAYER—AUTONOMOUS CONTROL SYSTEM

The coordination layer of the TCR autonomous control system includes sensors, actuators, and control system hardware and software that implement the finite state machine to perform higher level control functions. Unlike the continuous-time-domain actuations performed in the functional layer, the control functions in this layer are intended for major operational changes such as transition from one mode of operation to another. Operating modes and the associated mode transitions are the standard means of achieving plant startup and shutdown. These modes and transitions are highly proceduralized, labor intensive (in large nuclear power plants) and time-consuming activities.

Targeting higher-level control functions with a scope on mode transitions is useful for two reasons:

1. It provides a vehicle for demonstrating the autonomous control functionality, and
2. It provides a reasonable scope for the demonstration of autonomy without creating undue technical risks and potential regulatory risks for the TCR program.

The finite state machine model intended to generate the high-level supervisory control instructions can be implemented on an FPGA device. FPGAs are digital devices, but since they do not run an operating system kernel, their performance cannot be degraded by interrupt calls or other features that exist in computer-based programmable devices. These features make FPGAs an excellent candidate for applications in which time determinism is critical. Moreover, certain classes of FPGAs are not reprogrammable, making them more attractive from a cybersecurity perspective. The details of this implementation and the necessary hardware specifications to meet the performance requirements will be investigated during the initial development phase of the coordination layer.

4.3.1 Systems, Subsystems and Components

The coordination layer will be responsible for controlling the Tier-II systems. The list of systems, subsystems, and components in this tier will be identified through an iterative process as the TCR design and concepts of operation are developed.

4.3.2 Finite State Machine

As discussed in Section 2.8, the finite state machine approach offers a balance between performance and risk. Furthermore, finite state machine models are capable and in fact are more suited for mathematical representation of complex engineering procedures. The rich mathematical foundation available for the automata theory also provides confidence for testability and qualification. For instance, the regular language formalism of a supervisory control system exploits the best features of *regular expressions*. This provides a compact, *finite* representation for potentially complex languages with an infinite number of strings.

The power of finite-state-machine-based autonomous control can be illustrated in the following example.[36] Here, a portion of a heating system is considered which consists of a pump, valve, and controller, together with one valve flow sensor and a pump pressure sensor, as shown in Figure 7. The model of the valve accounts for possible failure modes in states defined as for *stuck closed* (SC) and *stuck open* (SO). The fault events `stuck_closed` and `stuck_open` that take the valve to the SC and SO states are assumed to be unobservable.

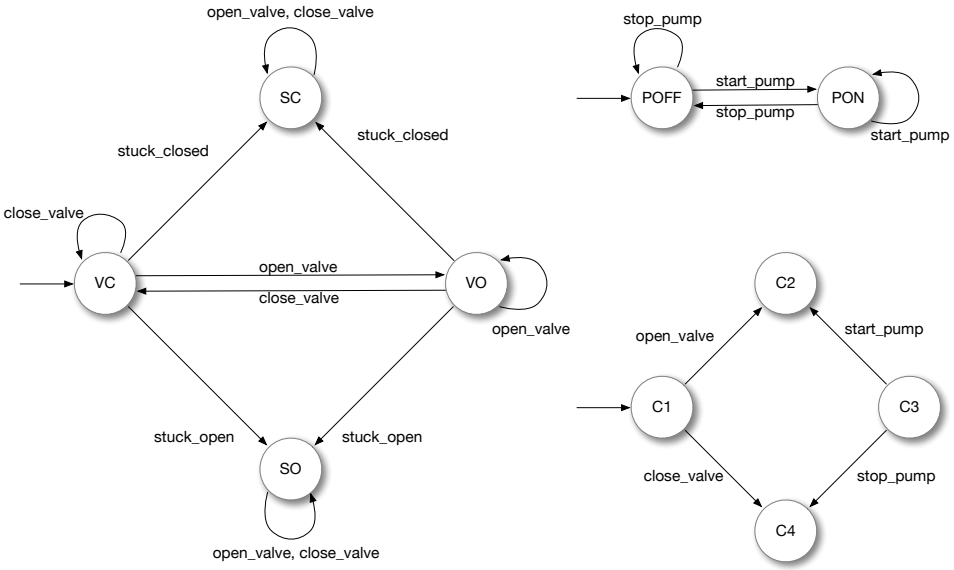
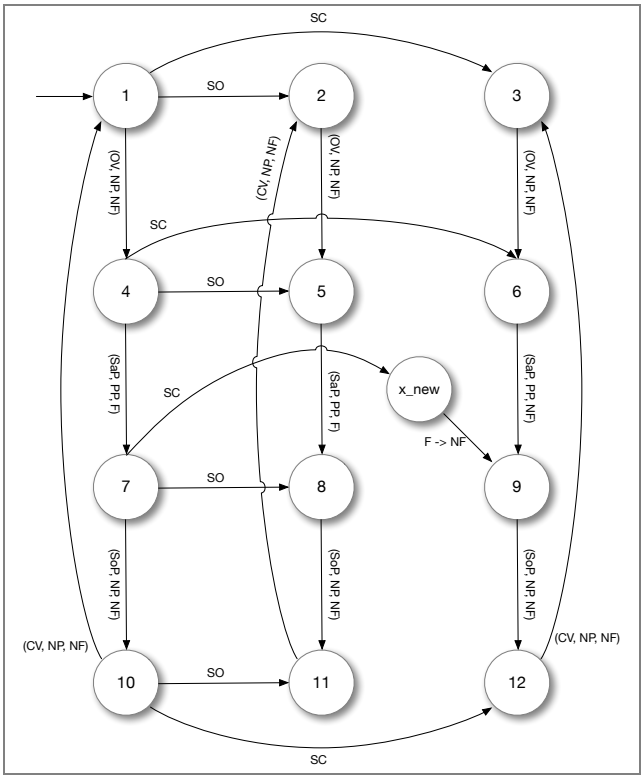


Figure 7. Individual finite state machine component models for pump, valve, and controller [adapted from Ref. 33].

The parallel composition of the three automata in Figure 7 is an automaton with twelve reachable states (Figure 8) with the discretized outputs of the sensors (see the inset table and legend).

[36] C. G. Cassandras, S. Lafortune, *Introduction to Discrete Event Systems*, Kluwer Academic Publishers (1999).



State No.	State name	Sensor readings
1	(POFF, VC, C1)	NP, NF
2	(POFF, SO, C1)	NP, NF
3	(POFF, SC, C1)	NP, NF
4	(POFF, VO, C2)	NP, NF
5	(POFF, SO, C2)	NP, NF
6	(POFF, SC, C2)	NP, NF
7	(PON, VO, C3)	PP, F
8	(PON, SO, C3)	PP, F
9	(PON, SC, C3)	PP, NF
10	(POFF, VO, C4)	NP, NF
11	(POFF, SO, C4)	NP, NF
12	(POFF, SC, C4)	NP, NF

Legend

POFF:	Pump OFF
PON:	Pump ON
CV:	`close_valve`
OV:	`open_valve`
SC:	`stuck_closed`
SO:	`stuck_open`
SaP:	`start_pump`
SoP:	`stop_pump`
VC:	Valve Closed
VO:	Valve Open
F:	Flow
NF:	No Flow
PP:	Positive Pressure
NP:	No Pressure

Figure 8. Complete finite state machine model of pump, valve, and controller with flow and pressure sensor (left); sensor map for the pump-valve-controller (right) [adapted from Ref. 33].

While the example appears to be trivial for a simple control unit, the mathematical tools made available by *regular languages* under the finite state automaton modeling approach provide a robust method to ensure that the total integrated system with the supervisory feedback control system (in the discrete-event sense) exhibits a behavior that prohibits any undesired states. For instance, these undesired states could be those where the system ends up in a block via deadlock or livelock; or they could be states that are physically inadmissible, such as starting up a pump without building up adequate hydraulic pressure for the seals. Moreover, a series of certain actions may violate a desired ordering of events, such as opening a flow valve before initiating a pump startup sequence.

The control paradigm is as follows. The state transition function of the system G can be controlled or modified by the supervisor S, in the sense that the controllable events of G can be *dynamically* enabled or disabled by S. Certain actions or events in the active event set in G cannot be executed unless that event is also included in $S(s)$.

4.4 ORGANIZATION LAYER—AUTONOMOUS CONTROL SYSTEM

The organization layer is reserved for more complex decision-making algorithms that rely on search-based methods such as dynamic programming, as previously discussed. Currently, no decision has been made regarding the implementation details of this layer. As the TCR design matures, an experiment plan may be developed to demonstrate the true decision-making capability in an autonomous control system.

5. ENABLING TECHNOLOGIES FOR TCR AUTONOMOUS CONTROL

As discussed in the previous sections, technologies that need to be integrated for autonomous control include measurements from multiple sensors, data analytics algorithms, and control and coordination methods.

5.1 EMBEDDED SENSING

Autonomous control implies decision-making, and decision-making requires abundance of data to make informed decision and to take proper actions. While there are technically sounds methods to infer unmeasured variables—Kalman filters being one of the most widely used techniques—these approaches bring about large uncertainties due to unmodeled dynamics or sometimes due to nonlinearities in the processes. Moreover, a linear time invariance assumption is hidden in most filtering approaches. These assumptions are valid about an equilibrium point. Therefore, during an operational transient such as a power ramp, the system goes through a range of equilibria around which distinct linearized models should be identified.

Conventionally, feedback control actions in large nuclear reactors are generated based on a few measurements—reactor bulk power and core average temperature being the most obvious ones. However, this fact should not be construed as a gap, but rather as a natural manifestation of the control problem. A large LWR, for instance, offers only reactivity control rods as an actuation interface on the primary side as the primary means of maintaining reactor outlet temperatures, because the primary coolant pumps do not allow speed control. For reactor inlet temperature, feedwater heater flow rates and the steam generator recirculation ratio are the control variables. For advanced reactors such as HTGRs, circulator speed—thus the primary fluid flow rate—is an additional control variable, in addition to reactivity control.

Therefore, the natural question is, "*what is the benefit of ubiquitous sensing if it is not going to lead to a more granular control of the system?* The answer is more complicated, and in fact, it forms the basis of the proposed autonomous control framework.

First, small-size reactor cores such as that of the TCR do not provide copious internal space to allow placement of large quantities of sensors. In fact, the fundamental impetus of an additively manufactured core is to optimize the heat-generation (i.e., neutronics) and heat-rejection (i.e., thermal-fluidic) processes in a manner that cannot be accomplished via conventional manufacturing techniques. Therefore, to extract additional data from the core, embedded sensing emerges as a potential solution. Embedded sensing would prevent undesired obstructions in the internal flow path and would help realize the true benefits of an additively manufactured core. A simplified conceptualization of one potential TCR core configuration is shown in Figure 9 with complex internal coolant flow paths feeding into upper manifolds. This unorthodox topology does not lend itself to conventional instrumentation approach.

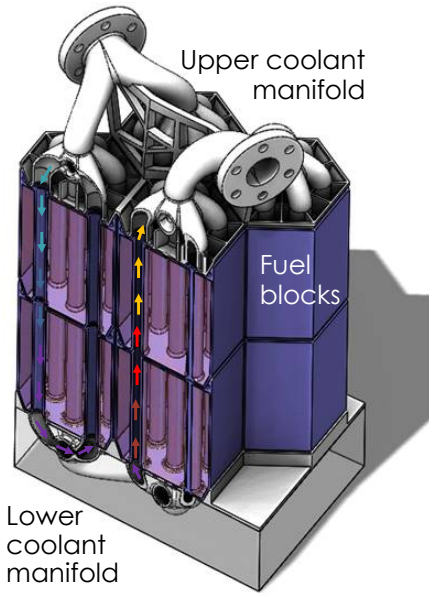


Figure 9. A simplified conceptualization of TCR core configuration with upper and lower coolant manifolds directing gas flow through fuel blocks stacked alongside one another.

Furthermore, within the context of autonomous control of TCR, there is a desire to monitor variables that indicate structural performance of additively manufactured components as a function of accumulated dose. As discussed previously, the TCR instrumentation strategy adopts a graded approach to minimize risk to the primary mission. Therefore, measurements that are directly connected to control or protection actions will be obtained using proven methods and components as previously deployed in previous high-temperature helium-cooled gas reactors. However, even with conventional instrumentation, the sensor placement strategy will be tightly coupled to the core and flow path design. The primary candidates for this approach are the placement of thermowells for temperature monitoring and plumbing of impulse lines for differential and gauge pressure monitoring. No direct flow measurement of the primary fluid was used historically in HTGRs despite its importance. Other than start-up and source-range, commercially available high-temperature compatible fission chambers will be used external to the reactor vessel.

Given the need to tightly couple sensors to the core and flow path design and the likely need to have a reasonable spatial density of sensors, embedding some of these sensors in the core and support structures during these components' additive manufacturing (AM) processes remains a possibility. The development of such embedded sensors is therefore an enabling technology for TCR and remains a focus area for R&D activities. Ongoing R&D activities are investigating the AM methods, but where needed, more conventional approaches such as welding and brazing can also be used. These alternative methods are considered a risk mitigation strategy for the necessary measurements for plant operation and safety.

5.1.1 Leading Measurement Modalities

Three measurement modalities stand out in the short term for embedded sensing:

1. embedded temperature sensing,
2. embedded strain sensing, and
3. embedded neutron flux and/or gamma field sensing.

Additionally, distributed monitoring of structural vibration and coolant flow may offer significant advantages.

5.1.1.1 Embedded Temperature Sensing

The rationale for in-situ temperature sensing through embedded instruments in additively manufactured structures is twofold: (1) having a spatially resolved temperature distribution has operational value for directly monitoring hot spots in critical structures, and (2) deviations from analytically—or computationally—predicted performance should provide insight into the evolution of thermal conductivity in additively manufactured components as a function of irradiation history.

While temperature sensing may be accomplished in a variety of ways, only a handful of technologies emerge as viable options in a high-temperature (~800°C) nuclear environment that are compatible with AM methods. Thermocouples have a demonstrated history and operational pedigree in high-temperature environments. The key focus area is the thermodynamic compatibility of thermocouple sheathing within the embedded host matrix. Therefore, the program is investigating this issue for ceramic materials and metals for a variety of sheathing alloys. For the sensing element, Type-N[37,38] and Type-K[39,40] thermocouples have demonstrated stability in thermal- and fast-spectrum nuclear applications. With proper selection of sheathing, embedding of qualified sensors appears to be a reasonable approach.

Likewise, embedded optical fibers can perform spatially distributed temperature sensing.[41] Figure 10 shows results from work being performed at ORNL, including a finished ultrasonic AM part with an embedded optical fiber that is flush with the surface of the part. Also shown is an optical micrograph of an embedded optical fiber with a copper coating (inset). Similar thermodynamic stability concerns apply to optical fibers and the necessary metal coating. The advantage of embedding optical fibers is that they do not require any additional wires for power.

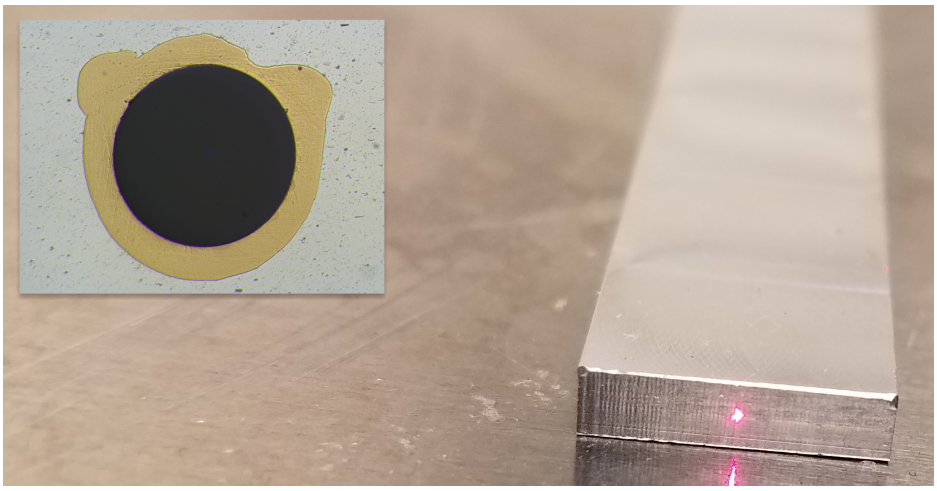


Figure 10. An embedded optical fiber (main); optical micrograph showing a copper-coated optical fiber embedded in aluminum (inset) [courtesy of C. Petrie, ORNL].

[37] K. Saito et al., "Instrumentation and Control System Design," *Nuclear Engineering and Design*, **233**(1–3), pp. 125–133 (October 2004).
[38] S. Shiozawa et al., "Overview of HTTR Design Features," *Nuclear Engineering and Design*, **233**(1–3), pp. 11–21 (October 2004).
[39] N. C. Hoitink, R. C. Weddle, and D. C. Thompson, "Effects of Fast Neutron Irradiation on the Performance Characteristics of Reactor-Grade Thermocouples," BNWL-1365, FFTF Project, Pacific Northwest Laboratories (June 1970).
[40] C. K. Day, "FFTF Core and Primary Sodium Circuit Instrumentation," HEDL-SA-1082, Hanford Engineering Development Laboratory (December 1975).
[41] T. W. Wood, B. Blake, T. E. Blue, C. M. Petrie, and D. Hawn, "Evaluation of the Performance of Distributed Temperature Measurements with Single-Mode Fiber Using Rayleigh Backscatter up to 1000°C," *IEEE Sensors Journal* **14** (2014) 124–128.

5.1.1.2 Embedded Strain Sensing

Embedded strain monitoring provides insight into the geometric evolution of the structure over the course of the operation of the facility and as a function of temperature history and accumulated dose. Strain monitoring is traditionally performed by using strain gauges. Fiber optics have also been proposed and demonstrated for strain monitoring. In addition to temperature sensing as previously discussed, embedded fiber optic sensors can perform spatially distributed sensing of strain.[42]

An important consideration when embedding for strain monitoring is the assurance of bonding between the sensor and the host matrix. Delamination during the lifecycle of the sensor due to differential expansion would essentially invalidate the strain reading. Therefore, the importance of bonding performance is more likely to be prevalent in this modality than others. As such, this program is placing significant emphasis on the quality of embedment and the examination of bonding performance after temperature cycling.

A second concern is the influence of temperature on the measured response. As described above, the measurement using optical fiber-based sensors is sensitive to temperature. When attempting to resolve the strain from the measured data, the effects of temperature must be deconvolved from the measurement. Methods exist for compensating for temperature in optical strain measurements,[43,44] so the R&D program will leverage existing approaches for this purpose.

5.1.1.3 Embedded Neutron Flux and Gamma Field Sensing

Self-powered neutron detectors (SPNDs) and self-powered gamma detectors (SPGDs) are common in-core diagnostic tools used for neutron flux and gamma field mapping in thermal nuclear reactors. SPNDs produce a proportional electrical current generated as a result of electrons stemming from neutron-capture reactions in the emitter that make it out to the collector. A generic SPND design is shown in Figure 11.

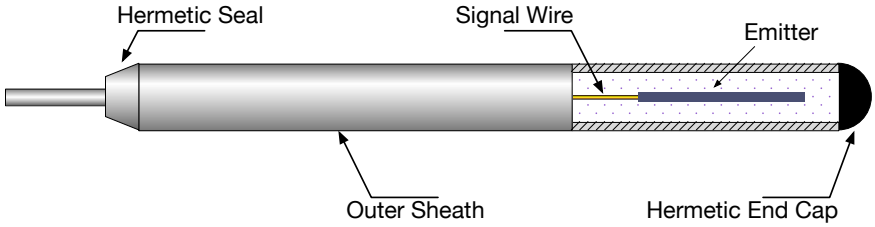


Figure 11. A typical self-powered neutron detector.

The two types of SPNDs are *delayed* and *prompt*. SPND type is determined according to the reaction mechanism for producing an electrical signal in the detector. Delayed-type SPNDs produce a signal through a (n, β) reaction during which an incident neutron is captured. The reaction product subsequently decays, emitting a β particle which exits the emitter and travels to the collector. In general, delayed-type SPNDs have the stronger signal per unit flux of the two SPND types, but the response time of the detector to changes in reactor flux is comparatively long, as it is limited by the half-life of the reaction product. Alternatively, prompt-type SPNDs generate an electrical current through a $(n, \gamma)(\gamma, e)$ reaction series in

[42] M. Froggatt and J. Moore, "High-spatial-resolution distributed strain measurement in optical fiber with Rayleigh scatter," *Applied Optics* 37 (1998) 1735–1740.
[43] M. R. Mokhtar et al., *Fiber-Optic Strain Sensor System with Temperature Compensation for Arch Bridge Condition Monitoring.* IEEE Sensors Journal, 2012. **12**(5): p. 1470–1476.
[44] Z. Zhou and J. Ou, "Techniques of temperature compensation for FBG strain sensors used in long-term structural monitoring." *Fundamental Problems of Optoelectronics and Microelectronics II*. Vol. 5851. 2005: SPIE.

which a neutron is captured and the resulting nucleus de-excites through a gamma-ray emission. Current is then produced when the resultant gamma-ray knocks an electron out of the neighboring atom and the subsequent capture of that electron in the collector. Prompt-type SPNDs respond instantaneously to changes in neutron flux, but they produce smaller signals per unit flux due to the necessity of two reactions occurring in tandem to generate a current. Commonly used collector and insulator materials are Inconel and MgO.

SPNDs and SPGDs have useful features for structural embedment purposes. First, they are relatively small, with diameters around 1.5 mm; the length of the sensing element may vary depending on the neutron flux and the desired sensitivity and statistical confidence for the measurement. Second, they are self-powered in that they do not require a bias voltage to operate, thus eliminating any additional high-voltage cables.

5.1.1.4 Structural Vibration Monitoring

Optical strain sensors may be used for vibration monitoring by monitoring the strain induced by vibration of the structure or component. Generally, such sensors use optical interferometry techniques to detect the phase changes induced in the optical signal due to strain. These optical interferometers are usually limited to monitoring vibration in a single location, although techniques to perform distributed vibration monitoring have been proposed.[45] The challenge with distributed sensing is the lower resolution and sensitivity.

As discussed in section 5.1.1.2, the TCR program is pursuing an R&D activity to embed optical sensors for strain monitoring during operation of the reactor. Assuming that questions on bonding of the sensor to the host matrix are resolved, these sensors are expected to have the necessary dynamic response to monitor low frequency (tens to hundreds of Hz) vibration induced by gas flow or other processes. This is an example of a single embedded sensor being used to monitor multiple quantities, and if successful, it will result in reducing the need for a dense set of embedded sensors.

5.1.1.5 In-Situ Flow Monitoring

The TCR program is pursuing an R&D activity to investigate the viability of helium flow velocity measurement based on acoustic emission. This transduction approach exploits the physic of fluid-structure interaction and the vortex shedding phenomenon that emerges as a result of encoded geometric features of a flow channel. The frequency of vortex shedding and coupled acoustic dynamics are proportional to the fluid velocity. This is an excellent example of embedded sensing in which the transduced waveform is directly modulated by the primary dynamics of interest, thus providing a direct indication of the process in the form of acoustic emission.

5.1.2 Monitoring of Non-Nuclear Components/Quantities

We place a specific emphasis on embedding sensor into in-core structures since advance manufacturing, the route we plan to exploit for the embedding process, is exclusively applied to the core. However, for more generic autonomous control applications, there are potential benefits in instrumentation of support systems and components—particularly rotating machinery such as pumps, components subject to high duty cycles such as valves, and connecting piping. These components have long been reported as a problem in the operation of nuclear facilities,[46] typically with higher failure rates, and as expected, with higher maintenance frequencies. A current challenge in existing nuclear power plants is that majority of

[45] C. Pan et al. *Opt. Express*, 25, 17, 20056–20070 (2017).
[46] Lydell, Bengt, and Jovica Riznic, "OPDE—the International Pipe Failure Data Exchange Project," *Nucl. Eng. Des.,* Vol. 238, 2008. doi:10.1016/j.nucengdes.2008.01.002.

the maintenance activities are planned based on a fixed schedule or on rough predictions based on the history of reported failures and frequencies. However, unanticipated failures of SSCs do occur, and they may cause significant loss of power generation, leading to loss of revenue. More ominously, it is proposed and anticipated that future reactors, particularly those to be deployed in micro-grid applications, are expected to be load followers, which significantly increases the lifetime duty cycle of these critical components. Therefore, more frequent failures should be expected, and the current reactive modus operandi (i.e., fail then fix) would be detrimental to the availability of a future advanced-reactor fleet.

Ongoing efforts in the nuclear industry to deploy online monitoring, diagnostics, and prognostics technologies (see Section 5.3) for existing plants are somewhat ad hoc, partly because these SSCs were not properly instrumented for this purpose during initial design and construction, and partly because of economic and regulatory uncertainties.

The leading online monitoring approach is vibration monitoring, which is typically accomplished by surface mounting a series of accelerometers. This is usually performed on rotating machinery or equipment that contains moving parts. Data analysis techniques, including frequency domain analysis methods, are typically used for analysis of the resulting measurements for detection and isolation of faults. Therefore, there is value in *deeply embedding* sensors into critical SSCs.[47]

5.1.2.1 Electrical Signature Analysis

Electrical signature analysis (ESA) is a versatile, powerful, nonintrusive technology for monitoring the health of electromechanical equipment. The diagnostic and prognostic information is acquired by installing voltage and current sensors on electrical lines carrying input or output power rather than requiring the placement of sensors on the equipment itself. In many industrial applications, these electrical lines are consolidated at the motor control center, which can be placed in a remote location from the equipment. Thus, an ESA-based monitoring system is intrinsically nonintrusive to equipment operations and provides remote monitoring capabilities.[48]

ESA was initially developed and applied by ORNL as part of the Nuclear Plant Aging Research (NPAR) program funded by the NRC[49] to (1) assess the effects of aging and service wear of selected nuclear power plant components and systems and (2) to identify condition monitoring methods that could be applied to maintenance, testing, and inspection activities to detect and mitigate the effects of aging prior to equipment failures.

It was later discovered that ESA methods could be useful in detecting and characterizing pump hydraulic instability, suction conditions, and other running load fluctuations.[50] It was noted that the time-dependent spectral features in the fluid pressure spectrogram were replicated in the pump motor power spectrogram. Other studies have shown that abnormalities and flow restriction changes in a pump loop can be detected and diagnosed by using ESA signatures.[51]

---

[47] It is important to make a distinction between critical components and safety or safety-related components. Here, the term *critical* is used in an informal manner to capture a component's significance in the overall availability of a plant. Obviously, safety or safety-related components are critical; but there are many non-safety–related components in a nuclear system whose availability may be a key determinant of overall availability.

[48] B. R. Upadhyaya, "In-situ Condition Monitoring of Components in Small Modular Reactors using Process and Electrical Signature Analysis," *NEUP Final Report*, Project No. 11-3212, University of Tennessee, Knoxville (December 2014).

[49] C. N. Obiozor, "Selection of Motor Operated Valves for Nuclear Power Plant Applications," *IEEE Explore*, 0-7803-2642 (1995).

[50] H. D. Haynes, "Electrical Signature Analysis (ESA) Developments at the Oak Ridge Diagnostics Applied Research Center," *Proc. COMADEM'95, 8th Int. Congress on Condition Monitoring and Diagnostic Engineering Management*, Kingston, Ontario, Canada (June 1995).

[51] H.D. Haynes, D.E. Welch, D.F. Cox, and R.J. Moses, "Electrical Signature Analysis (ESA) as a Diagnostic Maintenance Technique for Detecting High Consequence Fuel Pump Failure Modes," *Proc. 6th Joint FAA/DOD/NASA Conference on Aging Aircraft*, San Francisco, CA (September 2002).

While ESA has been shown to be a powerful diagnostics tool, when augmented with embedded sensors for monitoring key parts of electromechanical components such as bearings, gearboxes, or seals and gaskets, the prediction performance of diagnostics and prognostics tool is significantly boosted, directly pinpointing an impending failure. Obviously, design and fabrication of SSCs with embedded sensors must start early in the conceptual design phase of a component.

5.1.3 General Comments about Embedded Sensing

For both process and structural variables, measurements must be performed in situ during reactor operation. While there are a number of technologies for measurement modalities of interest that can provide the necessary information, challenges with embedded sensing within the core and core support structures must be resolved in a systematic manner through a series of laboratory tests, leading up to use in the demonstration platform.

A nuclear reactor core poses one of the most challenging environmental conditions of engineered systems, including sensors. Therefore, the process of sensor embedment must be investigated thoroughly for stability, reliability, and repeatability to gain confidence in the measurements. Moreover, there must be a path forward for standardization to ensure that the process of embedding delivers expected performance.

However, embedded sensing should not be interpreted as a panacea to all needs, gaps, and requirements for instrumentation. It is simply one of many tools in the toolset for measuring the necessary quantities and enabling the complex system engineering process for reactor design and deployment.

5.2 DATA ANALYTICS TECHNOLOGIES, DIAGNOSTICS AND PROGNOSTICS

Data analytics technologies are considered an enabling technology for autonomous control and operation. Broadly, these technologies can be categorized as technologies essential for the first demonstration of TCR startup and operation, and technologies that would be essential for future deployment of TCR at remote sites.

Essential data analytics and control technologies for the first TCR demonstration include technologies for online monitoring for sensor drift, as well as SSC diagnostics for plant state and control actuation confirmation. Developments that would be necessary for future remote deployment of TCR-like technologies include prognostic capabilities for assessing component condition and remaining service life.

5.2.1.1 Measurement drift due to sensor failure

Sensor drift that occurs due to aging or failure results in an inaccurate understanding of plant or system state. In safety critical systems, actuation actions taken as a result of incorrect information from aging or failed sensors can lead to catastrophic failure of systems. This occurs regardless of whether the actuation decisions are taken by an autonomous controller or by a human operator. However, the consequences may be magnified in an autonomous control setting by acting in ways that speed up system failure.

In LWRs, sensor aging, and failure generally occur over long periods of time with exposure to the reactor environment. Other causes of failure are usually due to manufacturing defects or incorrect maintenance procedures during activities such as sensor recalibration. In the TCR, given the limitations of existing sensor technologies for temperature and flow measurement for gas reactor environments,[52] sensor drift may occur over shorter time durations and will need to be identified quickly to ensure that faulty

[52] K. Korsah et al., "Assessment of Sensor Technologies for Advanced Reactors," ORNL/TM-2016/337, Oak Ridge National Laboratory, Oak Ridge, TN (August 2016).

measurement data are not incorporated into operational decision making. In addition, fault detection and diagnostics techniques are necessary to autonomously identify when the process begins to drift.

There are a number of algorithms for online monitoring (OLM) available for identifying sensor drift in a timely fashion[53,54,55]. In general, these techniques are data-driven and utilize models derived from training data to predict measurements under normal conditions, when there is no drift or process fault. Deviations from the predicted measurement indicate errors. Additional algorithms based on machine learning are generally applied for diagnostics.

In the present application, there is a lack of process data that may be used for developing the models. As a result, alternative approaches that rely on reduced-order models such as those developed using the TRANSFORM[56] package may be necessary.

5.2.1.2 Diagnostics of component state

Using diagnostics to determine a component's condition primarily involves an assessment of whether the component is functionally degrading. Diagnostics are generally performed by using measurements of one or more quantities that indicate component state. For example, bearing degradation in rotating machinery has been shown to result in the appearance of additional frequency components in vibration data.[57,58] The analysis methodologies for diagnostics are typically specific to the component and the measurement quantity.[59] However, these techniques may broadly be categorized into filtering and feature extraction, pattern recognition, and diagnostics.

Filtering and feature extraction methods are used to limit the effects of measurement noise on the diagnostic result. Most measurements are subject to various sources of noise, ranging from electronic noise to noise induced by process conditions such as flow-induced vibration noise in vibration measurements on active components. Filtering techniques limit the effects of noise outside the effective bandwidth of the measurement system and improve signal-to-noise ratio (SNR). Feature extraction methods help focus analysis methodologies on attributes that indicate degradation in the component. Feature extraction techniques can be time-series based, as in amplitude and rise or fall time, frequency based, as in peak frequency, amplitude at one or more frequencies, or full width at half maximum, or they can be joint time-frequency transform based. Also, statistical quantities such as the mean and variance of data within a time or frequency window are often computed from time, frequency, and time-frequency transforms of the measurements.

The actual analysis for diagnostics relies on the features computed from the data. Diagnostic algorithms include methods based on pattern recognition methods, including machine learning techniques, and correlation-based template matching approaches. Most such methods require a data set with known signatures of normal and degradation conditions, which may be difficult to obtain. Alternative model-

---

[53] Ramuhalli P, R Tipireddy, ME Lerchen, B Shumaker, JB Coble, AM Nair, and S Boring. 2017. "Robust Online Monitoring for Calibration Assessment of Transmitters and Instrumentation." In *Proc. ANS NPIC-HMIT 2017, San Francisco, June 11-15, 2017, pp. 1115-1124*.

[54] Hines, J.W. and E. Davis, *Lessons learned from the U.S. nuclear power Plant on-line monitoring programs.* Progress in Nuclear Energy, 2005. 46(3): p. 176-189.

[55] Hines JW, J Garvey, R Seibert and A Usynin. 2008. Technical Review of On-line Monitoring Techniques for Performance Assessment. NUREG/CR-6895, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, D.C.

[56] Fugate, D.L., et al., *Update on ORNL TRANSFORM Tool: Simulating Multi-Module Advanced Reactor with End-to-End I&C*. 2015, Oak Ridge National Laboratory.

[57] Koo, I.S. and W.W. Kim, *The Development of Reactor Coolant Pump Vibration Monitoring and a Diagnostic System in the Nuclear Power Plant.* ISA Transactions, 2000. **39**(3): p. 309-316.

[58] Tavner, P.J. *Review of condition monitoring of rotating electrical machines*. IET Electric Power Applications, 2008. **2**, 215-247.

[59] Agarwal, V., et al., "Application of data analytics for digital monitoring in nuclear plants," in *PNBC Conference*. 2018, ANS: San Francisco, CA.

based methods have been proposed in a few applications, especially for pump degradation quantification.[60]These methods develop a physics-based model of the component operation and use deviations from the model prediction to identify and diagnose degradation.

It is worth noting that such diagnostics technologies, especially for active components, are generally at a high technology readiness level (TRL) and are commercially available for some components. However, this is not the case for passive components, where the technology is still in the research phase (TRL 4–6). For the TCR, diagnostic information for active components is expected to be used in some of the autonomous control decisions. The system will use commercially available position indicators and vibration monitors for condition monitoring and the associated diagnostic algorithms for assessing component condition. In contrast, passive component diagnostics will be performed primarily to obtain insights into the performance of materials that are additively manufactured and in the initial phases of the demonstration, but this approach is not expected to be included in the control decisions.

5.2.1.3 Prognostics of SSC condition

Research at universities and national laboratories has led to a number of advances in analysis methodologies for diagnostics, prognostics, and supervisory control for improving the economics of advanced reactors.[61,59] While it is not necessary from the perspective of safely operating an advanced reactor such as the TCR, the reactor demonstration platform provides an opportunity for future testing, evaluation, and demonstration of some of these advances in technology. For example, demonstration of a vital set of tools for transforming advanced reactor economics is expected to be useful for industry and regulatory acceptance of such technologies for future commercial scale deployment of transformational advanced reactor concepts. Technologies of interest are as follows:

- Structural health monitoring and diagnostics for passive components
- Prognostics for SSC condition assessment and calculation of remaining service life
- Predictive control
- Fully autonomous resilient supervisory control

These technologies are especially of interest in smaller advanced reactor concepts where there is a relatively lower level of operational experience with the concepts when compared with LWRs. The associated limited level of knowledge about physics of failure mechanisms in these environments for some active and passive components makes it important to monitor the condition of these components in the first couple of demonstration reactors. The information from such condition monitoring and diagnostics/prognostics (i.e., estimation of the remaining service life of key components with some level of aging and degradation) can be an important element of control decision-making. Specifically, autonomous control systems can leverage information about component condition to determine whether an operational mode needs be changed to extend the life of the component to the next convenient outage.

Using reduced order plant model simulations and algorithms for prognostics, research[62] has demonstrated that the integration of these technologies can lead to improvements in plant up-time and can reduce maintenance-related shutdowns with no impact on safety. While they are not essential to the first demonstration of the TCR, these algorithms can be adapted and demonstrated on a subsequent run of TCR.

---

[60] Lee, J.K., et al., "Mathematical modeling of reciprocating pump," *Journal of Mechanical Science and Technology*, 2015. **29**(8): p. 3141-3151.
[61] Coble JB, P Ramuhalli, LJ Bond, W Hines, and B Upadhyaya. 2015. "A Review of Prognostics and Health Management Applications in Nuclear Power Plants." *Int'l. J. PHM*, 2015 016.
[62] Ramuhalli P, EH Hirt, G Dib, A Veeramany, CA Bonebrake, and S Roy. 2016. *Summary Describing Integration of ERM Methodology into Supervisory Control Framework with Software Package Documentation,* PNNL-25839 Rev. 0, Pacific Northwest National Laboratory, Richland, WA.

5.3 OTHER TECHNOLOGIES

With the focus of the control activity on the initial demonstration, I&C technologies that have been tried and tested in nuclear plants are planned for deployment. As envisioned, the RPS will be isolated from other systems and will include industry-standard practices for robustness, redundancy, and cybersecurity. Cybersecurity is likely to be a greater concern in future revisions of the reactor I&C that incorporate digital elements. Therefore, the initial I&C design does not address these emerging issues in great detail and only focuses on a view to identifying and documenting questions that must be addressed in the future.

6. SUMMARY

Autonomous control, when combined with the possibilities offered by advanced manufacturing methods, is expected to play a key role in enabling advances in the nuclear power area. However, the development and demonstration of autonomous operation in nuclear power plants requires the integration of sensing technologies, advances in data analytics, and the development of enabling technologies such as embedded sensors.

This report described a framework for autonomy in nuclear reactor operations, within the context of the TCR. An initial control strategy was outlined based on advances in autonomous operations in other application areas, and a number of enabling technologies identified for enabling autonomous operations of TCR.

This report offers the following key takeaway pertinent to our control strategy for TCR and demonstration of relevant, yet achievable advances towards autonomous nuclear energy systems:

- We conclude that discrete event models-based supervisory control approach offers the best near-term approach for the implementation of the TCR autonomous control system.
- The TCR I&C system design will adopt an approach that minimizes potential regulatory challenges regarding the implementation of the I&C platform.
- We will rely on conventional components and systems that have safety or safety-related functions.
- For the present application, autonomous operation focuses on moving the following human functions to algorithms:
    - step change in power level (increase or decrease) in response to a demand, and
    - slow ramp between two steady state operation modes.
- We will pursue three measurement modalities for embedded sensing:
    - embedded temperature sensing,
    - embedded strain sensing, and
    - embedded neutron flux and/or gamma field sensing.

We identify two phases in the development of technologies for achieving autonomy:

- The first phase focuses on quantifying process state and uses a coordination layer in the framework to determine actuation decisions to place the system in the desired state. Within each state, a classical control system is used to maintain the stability of the reactor.
- Future phases of development are expected to incorporate state of health into the decision making.

Ongoing research activities are focused on developing the necessary technologies for embedded sensing for key plant process variables along with specific state of health indicators. The control and coordination systems are also under development and will leverage design decisions as the TCR design matures.