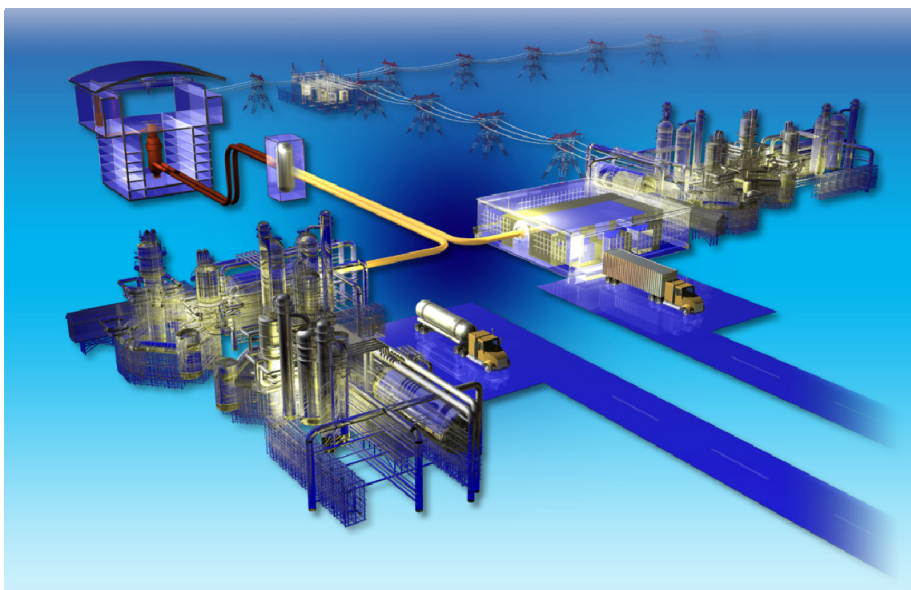


# HTGR Resilient Control System Strategy

September 2010

The INL is a  
U.S. Department of Energy  
National Laboratory  
operated by  
Battelle Energy Alliance



#### **DISCLAIMER**

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

# **HTGR Resilient Control System Strategy**

**September 2010**

**Idaho National Laboratory  
Next Generation Nuclear Plant Project  
Idaho Falls, Idaho 83415**

**Prepared for the  
U.S. Department of Energy  
Office of Nuclear Energy  
Under DOE Idaho Operations Office  
Contract DE-AC07-05ID14517**



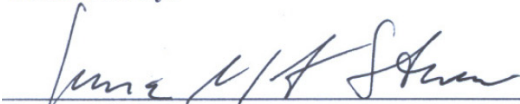
## Next Generation Nuclear Plant Project

# HTGR Resilient Control System Strategy


INL/EXT-10-19645  
Revision 0

September 2010

**Authored by:**

  
\_\_\_\_\_  
Lynne M. F. Stevens  
NGNP Systems Engineer

09 Sept 2010  
Date

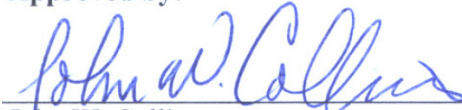
  
\_\_\_\_\_  
Craig G. Rieger  
ICIS Distinctive Signature Lead

09 Sept 2010  
Date

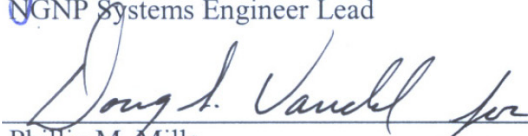
  
\_\_\_\_\_  
William C. Phoenix  
NGNP I&C Lead

09 Sept 2010  
Date

**Approved by:**

  
\_\_\_\_\_  
John W. Collins  
NGNP Systems Engineer Lead

09 SEPT 2010  
Date

  
\_\_\_\_\_  
Phillip M. Mills  
NGNP Engineering Director (acting)

09 Sept 2010  
Date

## SUMMARY

This document outlines the overall strategy for applying resilient controls to high temperature gas-cooled reactors (HTGRs) which is three fold:

- Protect the capital investment associated with key systems within each of the five plant areas.
- Enhance the efficient operation of key systems individually and collectively given the complex interactions across systems and areas.
- Identify and prioritize resilient functions for which HTGRs could most benefit from focused research and development, engineering analysis, and licensing awareness.

This report has been prepared for the Next Generation Nuclear Plant Project to provide the functional analysis of the current state of traditional control systems and that of resilient control systems; identify the gaps existing between traditional and resilient control systems that are most applicable to HTGR investment protection and operational efficiency; and, present the method to identify and rank, by risk reduction analysis, the most pressing resilient control system needs.

Industrial processes designed and built in the 1960s, 70s and early 80s typically employ analog instrumentation with automation to the extent allowed by such systems. With the growth in digital technologies and obsolescence of analog instruments and controls, industrial plant have retrofitted to digital instrumentation either plant-wide or one system at a time. This method of implementation lends itself to employing islands of automation with limited inter-connectivity and limited ability to control complex interactions between systems. The current fleet of Light Water Reactors (LWRs), similar to U.S. industrial plants built during the same period, employ a mix of analog and digital instrumentation and controls (I&C). Safety significant systems use analog instrumentation, and balance of plant systems have often been upgraded to digital I&C. With HTGRs in the early phases of design, opportunities exist to provide an integrated approach to plant instruments, controls, and automation.

Unlike traditional control systems, resilient control systems of the future will be designed, installed, operated, and maintained to survive a natural disaster, human error, or intentional cyber attack with no loss of critical function. This is no small challenge in a sector that is complex, highly networked, and sensitive to the mildest failure. To achieve resilience and address the threats in next generation control systems, research is required to integrate an understanding of cyber security, human interaction, and complex network design. The integration of these three aspects will be introduced in the concepts of data fusion, mixed initiative, and hierarchical control system design.

A resilient system can be defined as “one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.”<sup>5</sup> The framework for a resilient control system contains principles and methods that proactively recognize threats, integrate automation and human response, provide robust and adaptive mechanisms, consider all threats and events, and tailor information to the consumer. These methods and principles improve a system’s ability to anticipate, perceive, respond and adapt. Improvements to these four abilities increase the system’s overall ability to perform its necessary functions and operate resiliently. As this report shows, control systems with adequate levels of resilience perform at higher levels and respond more quickly to disturbances.

The key features of a resilient control system are state awareness of all plant systems and their interactions for resilient design. State awareness for all plant systems and interactions is the top down view where understanding exists of all aspects that may affect performance, including stability, efficiency, physical security, and cyber security. Design for resilience is a bottom up view, where the inherent design of the system is built to account for the areas of resilience. These areas of resilience are human systems, cyber awareness, and complex networked-control systems. Although additional areas of resilient controls are applicable to HTGR, this report focuses on key areas without listing the entire set of

resilient controls areas and features. A notional measure of resilience is in the adaptive capacity, or the ability to respond to a threat and maintain acceptable functionality.

An analysis of specific HTGR applications of resilient controls indicates additional research opportunities to advance the state of practice in resilience and prepare resilient methods for use in HTGRs. Resilient research areas of particular interest to HTGR investment protection include:

- Cyber and physical security,
- Process stability and efficiency,
- Integration of diverse indicators, and
- Interlacing of human and automatic responses.

This report also provides specific scenarios where resilient controls will influence HTGRs by showing that control systems with adequate levels of resilience perform at higher levels, respond more quickly to disturbances, provide more efficient operations, and increase public protection.

# CONTENTS

SUMMARY .....	iv
ACRONYMS.....	viii
1. INTRODUCTION .....	1
1.1 Resilient Control .....	2
1.2 Attributes of Resilient Systems.....	3
1.2.1 Anticipate .....	3
1.2.2 Perceive.....	3
1.2.3 Respond.....	4
1.2.4 Adapt.....	4
1.3 Areas of HTGR .....	4
2. STRATEGIC PURPOSE.....	5
3. HTGR APPLICABLE OPPORTUNITIES .....	6
3.1 Scenario 1: Undetected changes or lack of awareness of plant condition.....	6
3.2 Example Scenario 2: Inference of Parameters Not Directly Measured.....	6
3.3 Example Scenario 3: End User Induced Transients .....	7
3.4 Scenario 4: Cyber Attack .....	8
3.5 Scenario 5: Safeguards/Nonproliferation.....	8
3.6 Scenario 6: Disruption in Power .....	9
3.7 Scenario 7: Steam Generator Leaks .....	10
3.8 Benefits to HTGRs – Filling the Gap between Resilient and Traditional Controls .....	10
4. TRADITIONAL CONTROL SYSTEMS .....	11
4.1 Traditional Control System Functional Framework and Definitions.....	11
4.2 Traditional Control System Functional and Operational Flow .....	13
5. RESILIENT CONTROL SYSTEMS .....	14
5.1 Resilient Control System Functional Framework and Definitions .....	15
5.1.1 Monitor System Functional Additions.....	16
5.1.2 Manage and Process Data Functional Additions .....	17
5.1.3 Provide Systems Communications Functional Additions.....	18
5.1.4 Manage Control Processes Functional Additions .....	19
5.2 Resilient Control Functional and Operational Flow .....	19
6. HTGR APPLICABLE FUNCTIONAL GAP ANALYSIS.....	21
6.1 Monitor System Gap Analysis .....	21
6.2 Manage and Process Data Gap Analysis.....	23
6.3 Provide Systems Communication Gap Analysis.....	24
6.4 Manage Control Processes Gap Analysis .....	25
7. STRATEGIC PATH FORWARD TO FILL THE GAP .....	27



7.1	Gaps and Research Needs .....	28
7.2	Method of Identifying Most Pressing Needs .....	29
7.2.1	Risk Reduction.....	29
7.2.2	Rating of Resilient Features .....	30
7.3	On-Going Research.....	32
7.3.1	Resilient Control System Network Agents .....	32
7.3.2	Wireless Sensor Testing.....	32
7.3.3	Integrated Control System Data Fusion .....	32
7.3.4	Anomaly Detection, Diagnosis, and Resilient Control in Complex Engineered Systems .....	33
7.3.5	3-D Spatial Representation in Support of Design Inspection & Verification .....	33
7.3.6	Resilient Condition Assessment Monitoring (ReCAM) System.....	33
7.3.7	Automated Differential Equation-Based Identification .....	33
8.	CONCLUSION .....	34
9.	REFERENCES .....	35

## FIGURES

Figure 1.	Control system performance level vs. time. ....	3
Figure 2.	NGNP Architecture. ....	4
Figure 3.	Traditional controls functional framework.....	12
Figure 4.	Traditional controls functional flow. ....	13
Figure 5.	Traditional control system operational flow.....	14
Figure 6.	State awareness, resilient design, and threats. ....	15
Figure 7.	Resilient control system.....	16
Figure 8.	Functional additions of resilient control systems. ....	18
Figure 9.	Resilient control system operational flow. ....	20
Figure 10.	Gap analysis process.....	21
Figure 11.	Monitor System with Resilient Features.....	22
Figure 12.	Manage and Process Data with Resilient Features. ....	23
Figure 13.	Provide Systems Communications with Resilient Features. ....	24
Figure 14.	Manage Control Processes with Resilient Features.....	26
Figure 15.	Resilient Control System Path Forward. ....	28
Figure 16.	Resilient Features Scoring. ....	31

## TABLES

Table 1.	Identified Key Systems and Components for Each Plant Area.....	5
Table 2.	Key Systems, Components, and Resilient Controls Research Areas.....	28

## ACRONYMS

AC	Alternating Current
AQ	Assessment Quality
BOP	Balance of Plant
DC	Direct Current
DIV	Design Information Verification
FIS	Facility Information System
FOAK	First of a Kind
GAO	Government Accountability Office
HPS	Hydrogen Production System
HTGR	High Temperature Gas-Cooled Reactor
HTS	Heat Transport System
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Controls
IHX	Intermediate Heat Exchanger
INL	Idaho National Laboratory
IP	Internet Protocol
IQ	Information Quality
IT	Information Technology
LOHS	Loss of Heat Sink
LWR	Light Water Reactor
NGNP	Next Generation Nuclear Plant
NHS	Nuclear Heat Supply System
NRC	Nuclear Regulatory Commission
PCS	Power Conversion System
RF	Radio Frequency
ROT	Reactor Outlet Temperature
RPV	Reactor Pressure Vessel
SG	Steam Generator
SysID	System-Identification
THTR	Thorium High Temperature Reactor
UPS	Uninterruptible Power Supply



# HTGR Resilient Control System Strategy

## 1. INTRODUCTION

Control Systems and their associated instrumentation must meet reliability, availability, maintainability, and resiliency criteria for high temperature gas-cooled reactors (HTGRs) to achieve high capacity factors and remain economically competitive. Resilient control systems are one way of achieving the required availability by providing state awareness of all plant systems and their interactions and operational normalcy to allow for high capacity factors. The capacity factor is the total energy the plant produced during a period of time divided by the energy the plant would have produced at full capacity during the same period of time. This report supports the development of an overall strategy for applying resilient controls to HTGRs by showing that control systems with adequate levels of resilience perform at higher levels, respond more quickly to disturbances, increase operational efficiency, and increase investment and public protection. This report, along with the *Next Generation Nuclear Plant Resilient Control System Functional Analysis*<sup>4</sup>, functionally analyzes the gaps between traditional and resilient control systems as applicable to HTGRs. This report defines resilient controls, assesses the current state of both traditional and resilient control systems, documents the functional gaps existing between these two controls approaches as applicable to HTGRs, presents scenarios where resilient controls will greatly benefited nuclear systems, and discusses how resilient control system features become mitigation strategies for reducing risk. This document also identifies and prioritizes resilient functions for which HTGRs could most benefit from focused research and development, engineering analysis, and licensing awareness.

Industrial processes of the past typically employ analog instrumentation with automation to the extent allowed by such systems. With the growth in digital technologies and obsolescence of analog instruments and controls, industrial plant have retrofitted to digital instrumentation either plant-wide or one system at a time. This method of implementation lends itself to employing islands of automation with limited inter-connectivity and limited ability to control complex interactions between systems. The current fleet of Light Water Reactors (LWRs), similar to U.S. industrial plants built during the same period, employ a mix of analog and digital Instrumentation and Controls (I&C) with mainly off the shelf components. Safety significant systems use analog instrumentation, and balance of plant systems have often been upgraded to digital I&C, some with advanced, separate from the system, bolt-on measures such as cyber security. With HTGRs in the early phases of design, strategic opportunities exist to provide an integrated, global approach to plant instruments, controls, and automation for increased efficiency and investment protection.

Unlike traditional control systems, resilient control systems of the future will be designed, installed, operated, and maintained to survive a natural disaster, human error, or intentional cyber attack with no loss of critical function. Resilient control systems of the future will also migrate from bolt-ons to a holistic integration of key areas such as cyber security. This is no small challenge in a sector that is complex, highly networked, and sensitive to the mildest failure. To achieve resilience and address the threats in next generation control systems, research is required to integrate an understanding of cyber security, human interaction, and complex network design. The integration of these three aspects will be introduced in the concepts of data fusion, mixed initiative, and hierarchical control system design.

This report also provides specific scenarios where resilient controls will influence HTGRs by showing that control systems with adequate levels of resilience perform at higher levels, respond more quickly to disturbances, provide more efficient operations, and increase public protection. A resilient strategy seeks to improve availability and enhance the economic competitiveness of the plant.

## 1.1 Resilient Control

A resilient system can be defined as “one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.”<sup>5</sup> The key features of a resilient control system are state awareness of all plant systems and their interactions and design for resiliency. State awareness of plant systems and their interactions is the top-down view, where understanding exists of all aspects that may affect performance, including stability, efficiency, physical security, and cyber security. Resilient design is a bottom-up view, where the inherent design of the system is built to account for the areas of resilience, including human systems, cyber awareness, and complex networked-control systems. A notional measure of resilience is in the adaptive capacity, or the ability to respond to a threat and maintain acceptable functionality.

A preeminent objective for corporate and government organizations is the protection of major investments, which is attained by achieving state awareness, a comprehensive understanding of security and safety, for critical infrastructures.<sup>1</sup> Given the dependence of critical infrastructure on control systems for automation, the integrity of these systems and their ability to provide owner/operators a high degree of state awareness is essential in attaining a high degree of investment protection and public acceptance. Operators as well as government are, therefore, burdened to ensure they have a timely understanding of the status of their plant or all plants, respectively, to ensure efficient operations and investment and public protection. “This characterization is a significant objective that must consider many aspects of instrumentation, control, and intelligent systems in order to achieve the required result. These aspects include sensory, communication, analysis, decision, and human system interfaces necessary to achieve fusion of data and presentation of results that will provide an understanding of what issues are important and why.”<sup>2</sup>

An example of the need for resilient controls is found in the loss of Air France Flight AF447. The loss of reliable speed indication led to the disaster. A resilient control system might, in theory, determine the confidence in the reliability of pitot tube signals (maintaining state awareness) being used to control the airplane and replace them with other signals, for instance from a multiple global positioning system or other signals, until the pitot tubes returned to being reliable. Research that might benefit the aircraft and other industries, such as the nuclear industry, could include identifying strategies for determining the confidence of a group of similar primary instruments and diverse secondary instruments and the methodology and other details in replacing signals from the primary instrument with signals from the secondary instruments.

Resilience is key in quickly identifying threats, providing essential operational information, and providing an adaptive capacity for response. As this strategy shows, control systems with adequate levels of resilience perform at higher levels and respond more quickly to disturbances. Figure 1 shows that a resilient control system is more able to reduce the magnitude and duration of disruptive events. The effectiveness of a resilient system depends on its ability to anticipate, perceive, respond, and adapt to a potentially disruptive event. The increased performance over time provided by a resilient control system increases operational efficiency and public safety.

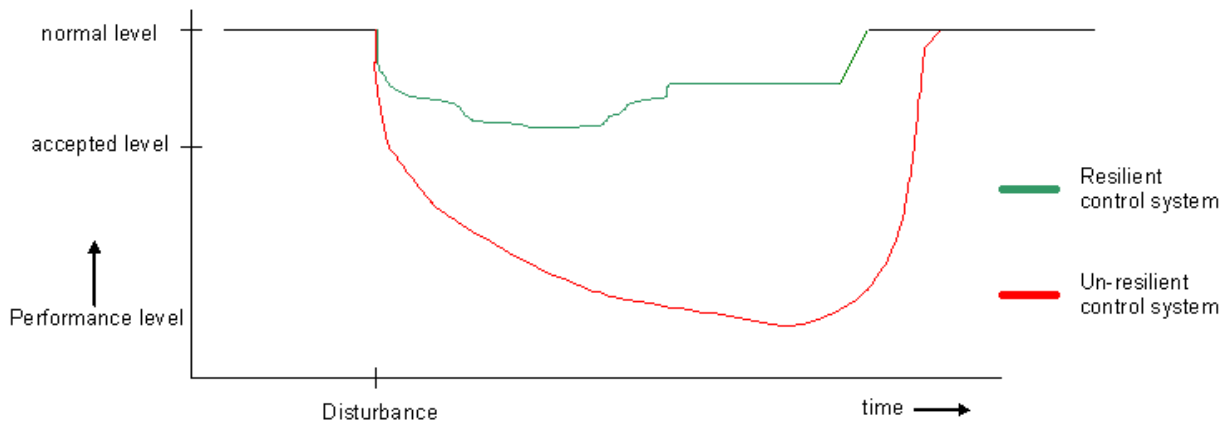


Figure 1. Control system performance level vs. time.

## 1.2 Attributes of Resilient Systems

To reduce process perturbations, a resilient system must reduce the likelihood of an adverse event such occurring and the severity of the consequence should the event occur. “A resilient system must have the ability to anticipate, perceive, and respond. Resilience engineering must therefore address the principles and methods by which these qualities can be brought about.”<sup>8</sup> In resilient systems, the probability is reduced with a system that ANTICIPATES the event and ADAPTS appropriately. The consequence is reduced with a system that PERCEIVES the event and RESPONDS appropriately. As any system’s ability to anticipate, adapt, perceive, and respond increases, so does the potential quality of its functioning in the face of disturbance, both expected and unexpected. Therefore, the potential resilience of the system increases. For this reason, the rating system is geared towards increasing the systems’ capabilities in these four areas of resilience.

### 1.2.1 Anticipate

A resilient system must have the ability to anticipate disturbances and threats. A given system feature contributes to the system’s ability to anticipate largely by enabling the system to be proactive instead of reactive and by helping the system to predict.

Many analog and digital control systems respond to changes in parameters, a form of feedback or reactive control, and present data in a retrospective manner. A resilient system could calculate the expected response of a system or collection of systems such as a power plant to a proposed control action, map and display to the operator the limits of anticipated acceptable response, conduct control operations after the operator gives the system permission to operate, and continue to display the behavior of the system and plant to ensure that the response of the plant is as expected.

### 1.2.2 Perceive

A resilient system must have the ability to perceive the state of equipment and threats to the system. A given resilient system feature contributes to the system’s ability to perceive when it helps the system to obtain correct information and knowledge about what is really going on in the system.

All instrument systems, including resilient systems, receive inputs from sensors. A resilient system will recognize the state of the equipment in the system and the overall operation of the system, including deviation from expected operation, from the sensor inputs. Beyond identifying deviations in equipment operation, it would be able to determine if inputs do not match the perceived state of the equipment or system or expected operation, an attribute that would help it identify, for instance, unauthorized access and manipulation of a digital control system.

### 1.2.3 Respond

A resilient system must have the ability to respond to what it perceives in an accurate and timely manner. When the system achieves state awareness, it must understand the meaning of that state and be ready and able to act.

The resilient system would have the ability to respond, or not, to changes in input sensor values depending on if it determines the values to be accurate and if the response is appropriate. It would have the ability to alert the operator to normal and adverse operation of equipment and system responses, and intrusions into the control systems.

### 1.2.4 Adapt

A resilient system must have the ability to respond to that which it anticipates. This ability is defined as adaptation and includes adjustments to processes and output signals in light of the anticipated disturbance.

Resilient systems have adaptive capacity. Adaptive capacity is the measurement of the buffer the system has between full operability and minimum acceptability. Since not all occurrences can always be predicted, this buffer will benefit unexpected events by providing a mechanism to enhance the assurance that the minimum system will maintain operation during expected and unexpected events.

In the example listed above, the resilient control system might anticipate when the system or plant is deviating from the predicted response and alert the operator or adapt control functions such as gains, an adaptive response, to ensure that the system or plant continues to operate acceptably.

## 1.3 Areas of HTGR

The NGNP can be divided into five areas: Nuclear Heat Supply System (NHS), Heat Transport System (HTS), Hydrogen Production System (HPS), Power Conversion System (PCS), and Balance of Plant (BOP). Each area is further broken down into systems, which are comprised of subsystems, which are further comprised of components as shown in Figure 2. Given the five areas for the NGNP, selected systems and components were identified for each area required to perform the desired functions and meet the needs specified by the project which would benefit from resilient control as shown in Table 1.

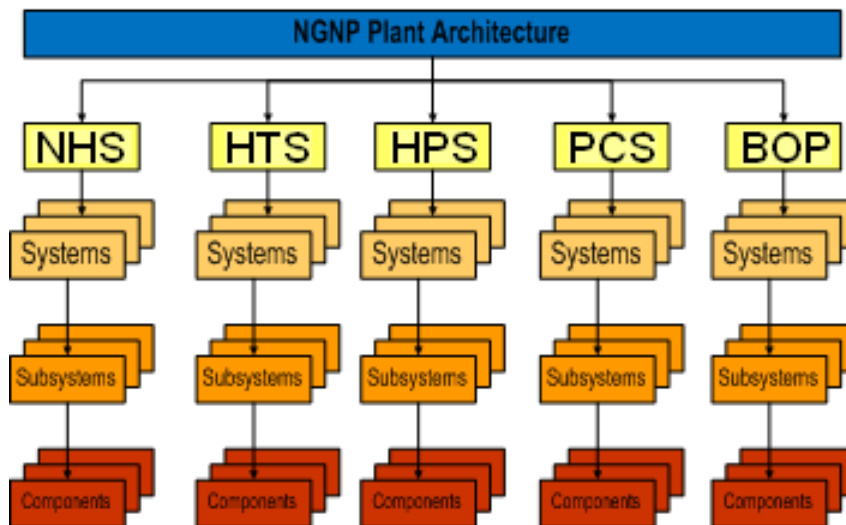


Figure 2. NGNP Architecture.

Table 1. Identified Key Systems and Components for Each Plant Area

Areas	Selected Systems and Components
<b>Nuclear Heat Supply</b>	Reactor Pressure Vessel (RPV)
	Reactor Vessel Internals
	Reactor Core & Core Structure
	Fuel Elements
	Reserve Shutdown System
	Reactivity Control System
	Core Conditioning System (Shutdown Cooling)
	Reactor Cavity Cooling System
<b>Heat Transport</b>	Intermediate Heat Exchangers (IHX)
	Steam Generator (SG) (for 750°C ROT)
	Circulators
	Cross Vessel
	High Temperature Valves (Isolation, Flapper, & Relief) Mixing Chamber
<b>Hydrogen Production</b>	High Temperature Steam Electrolysis
<b>Power Conversion</b>	Steam Generator (for 950°C ROT) Power Conversion System (PCS)
<b>Balance of Plant</b>	Fuel Handling System
	Instrumentation and Control
	Power Supply
	Physical Plant Security

## 2. STRATEGIC PURPOSE

The purpose of this document and the strategic purpose in applying resilient controls to HTGRs is three fold:

- Protect the capital investment associated with key systems within each of the five plant areas.
- Enhance the efficient operation of key systems individually and collectively given the complex interactions across systems and areas.
- Identify and prioritize resilient functions for which HTGRs could most benefit from focused research and development, engineering analysis, and licensing awareness.

Systems and components within each of the HTGR plant areas represent a large capital investment and are susceptible to useful life reduction due to fatigue and thermal cycling. Systems and components, such as the RPV, IHX, and SG, are investments that can be protected through steady state operation and limited thermal cycling.

Perturbations in end-use applications can introduce system transients throughout the plant up to and including the IHX and RPV. Due to the complexity in system interaction, advanced and resilient controls can enhance efficiency, enhance performance, and reduce perturbation induced thermal cycling.

Resilient functions that can benefit HTGR in this way need to be further developed for successful implementation in HTGRs. Research and development and engineering analysis performed by universities, national laboratories, and industry should be directed to address these resilient functions.



To achieve this stated purpose, HTGR applicable opportunities are presented (Section 3); a functional analysis of the current state of traditional control systems (Section 4) and a functional analysis of the current state of resilient control systems (Section 5) was performed; gaps between traditional and resilient control systems were identified (Section 6); a method to prioritize those gaps with the greatest applicability to HTGR investment protection and operational efficiency is presented (Section 7). By furthering the state of the art in resilient controls and implementing selected resilient functions in HTGR design, it is anticipated that HTGRs will employ control systems that perform at higher levels, respond more quickly to disturbances, provide more efficient operations, and increase protection of these investments.

### **3. HTGR APPLICABLE OPPORTUNITIES**

A resilient control system considers all threats and events by which proper operation is determined. A hierarchical control system design provides a robust and adaptive mechanism for optimizing control system performance to measures of normalcy. The seven notional scenarios presented and the discussion that follows illustrate the benefits and gains that moving from traditional controls to resilient controls will bring to HTGRs.

#### **3.1 Scenario 1: Undetected changes or lack of awareness of plant condition**

HTGR Area of Applicability: NHS, HTS, PCS

The HTGR will operate at higher temperatures than the current fleet of reactors for months at a time and the temperature sensors for the hottest gas temperatures could drift, perhaps significantly, or might fail completely. It is anticipated that hot gas temperature measurements will be required by the control systems which could operate to protect equipment such as the Intermediate Heat Exchanger and Steam Generator from excessive temperatures, changes in temperature, or other off-nominal and potentially damaging operation. Current approaches to reactor protection and control rely on parameters being sensed by instruments whose uncertainty includes a predicted amount of drift. Drift is a time-dependent change in a sensor's reading. The outright failure of certain sensors, for instance due to vibration, or excessive drift, has resulted in plants being shut down to replace the sensors.

Resilient control might perceive that sensors had failed or excessively drifted, respond by identifying the failure to the operator, identify potential consequences by anticipation, and permit continued operation by adaptation. The adaptation might include replacing the signal from failed or excessively drifted sensors with inferred parameters based on other sensors that are known to be valid, coupled with models of the operation of various components such as the intermediate heat exchanger and steam generator.

#### **3.2 Example Scenario 2: Inference of Parameters Not Directly Measured**

HTGR Area of Applicability: HTS and PCS

The steam generator of the HTGR will likely be comprised of tubes of different metals, joined by a dissimilar metal weld. The weld is intended to operate in superheated steam rather than subcooled or saturated water. The point in the tube where saturated steam becomes superheated depends on many parameters including reactor power level, gas flow rate and temperatures, feedwater flow rate and temperature, steam pressure, and the degree of superheat in the steam exiting the steam generator, all of which reflect the varying local heat transfer along the steam generator tubes. The amount of superheat in the steam exiting the steam generator is used to control the amount of water in the steam generator and, by extension, the location where saturated steam dries and becomes superheated.

In an actual steam generator, the tubes might not all be the same length and there might be other differences. Furthermore, one or more steam generator tubes might be restricted which would change the temperature distribution, and to some extent the flow, of coolant within the steam generator.

Factors contributing to aging and degradation of the steam generators throughout a fuel cycle and for the life of the generators include deposition of water-side chemicals (fouling) that decreases local heat transfer and, because they are likely to be deposited in the subcooled and boiling regions, shift the transition from saturated to superheated steam and the shift might be different for various tubes. Leaking tubes could be restricted, thereby changing the distribution of hot gas and water and steam within the steam generator. It will likely be important for a control system to infer the superheat boundary and ensure that it remains below the dissimilar weld.

Resilient control might perceive the presence, extent, and result of fouling from values provided by a variety of sensors. It would respond by identifying the fouling to the operator and other interested parties such as maintenance and engineering, provide a graphic view of super heat boundary location, identify potential causes and anticipate consequences of operation including the potential for damage to the weld or downstream components by continued operation, and permit continued operation by adaptation of control settings. Developing the supporting knowledge base for such a resilient control system would probably require studies by a sophisticated thermal hydraulic model of the steam generator and its interactions with the flow patterns and temperatures of the primary coolant. The model would probably require benchmarking, for example as was conducted for the THTR steam generator where several steam generator tubes were instrumented with thermocouples in the gas and liquid adjacent to several tubes. Thermocouples could not be attached directly to the tubes, the ideal situation, for fear of compromising the integrity of the tubes. The comparison was made between predicted and measured temperatures to provide some assurance that the heat transfer calculations were correct; a similar exercise might be required on the first of a kind steam generator.

### **3.3 Example Scenario 3: End User Induced Transients**

#### HTGR Area of Applicability: NHS, HTS, PCS

The HTGR will likely react to changes in customer demand for heat or electricity in a load-following mode rather than in a purely baseloaded mode where it supplies a steady fixed amount of heat and electricity. Even if its operation is planned to be baseloaded, it must still be able to respond to severe changes in heat and electrical demand without tripping and recover and continue to support a customer. Any sudden loss of heat removal from the primary to the secondary system through the IHX can cause a Loss of Heat Sink (LOHS) event. Loss of load can be caused by a turbine or compressor trip as well as any other failure in the gas turbine. If not quickly mitigated, this will have a significant effect on cold leg components, and will raise the primary coolant pressure significantly. An LOHS event can also happen in a steam cycle configuration through a loss of steam generator cooling due to loss of water/steam flow, spurious closure of secondary (water side) isolation valves, or steam/water leakage.

The worst case unmitigated scenario would suggest that the primary coolant temperature would eventually reach reactor core outlet temperature and be transferred to the reactor core inlet. This represents a very large temperature rise, which would be coupled with a primary pressure increase due to gas expansion. The IHX would also be quickly exposed to high helium temperatures at its outlet. The hot helium leaving the IHX and entering the reactor vessel as a minimum could reduce equipment life due to thermal excursion or cycling. In the worst case, equipment could be damaged and result in system unavailability.

The current generation of light water reactors have very limited load following capability and have little ability to survive severe grid disturbances.

Some of the large components in the HTGR may require significant evaluation to support approaches to minimize fatigue life usage i.e., intermediate heat exchanger and steam generator. The large

components could include the intermediate heat exchanger and steam generator. Fatigue usage due to large changes in temperature might result from rapid significant changes in heat demand. Such changes might occur if a valve controlling a significant amount of heat closes but then is reopened shortly thereafter. The thermal mass of the graphite in the reactor and the inherent characteristics of the HTGR core will likely reduce power as temperatures rise and then increase it as temperature falls again in response to the changing steam demands. The changes in secondary and primary temperatures and pressures might consume significant amounts of fatigue life, thereby shortening their projected lifespan.

A resilient design considers the overall efficiency and stability of the coupled processes holistically. In an accident scenario, an abnormal increase in primary temperature or pressure causes a reactor trip and automatic trip of the primary circulators to prevent the hot helium from reaching the reactor inlet. In a resilient control system design, advanced fault diagnosis and detection of all elements that characterize system health will be performed, and control changes or warning events are initiated as a result. Resilient detection systems, automatic trips, cooling systems, and alternate sources of heat sink all help mitigate the consequences of the event and minimize investment risk.

Resilient control, as a 'bottom-up' concept, can integrate the complex relationships of fatigue life usage, the changing demands of heat and electricity customers, and the limitations of the core and reactor to expand the range of operating conditions and limit transients. Integration of the limitations of every component and their complex interactions is beyond current control schemes whereas resilient control offers the potential for control by perceiving the state of the plant, anticipating future states with significant usage of fatigue life, responding in ways that limits fatigue usage, and if necessary adapting heat demand changes.

### **3.4 Scenario 4: Cyber Attack**

#### HTGR Area of Applicability: BOP/I&C

Cyber security is a significant concern for digital control systems. Most protections come in the form of passwords and network appliances, such as firewalls, routers, and switches. In addition, the networking protocols are based on standard Internet Protocol (IP) technology.

A hacker might be able to penetrate a nuclear plant's control system, trip the plant, or display false signals to a controller who then acts on them to trip the plant or damage equipment.

A resilient control system could potentially thwart displaying false signals or false control by perceiving that the signal being externally manipulated did not match the condition being supported by other sensors, identify the potentially false signal and the potential presence of an external threat to the operator, anticipate control actions that should not be taken, and adapt by replacing the signal with a valid one. The compromise need not be an external threat. It could be internal and not necessarily hostile. For example, it could result from a mistake by a trusted individual such as loading the wrong control algorithm into the computer. In a consequence-based, data fusion algorithm, critical and likely targets of compromise, such as the high-consequence lube oil system would be monitored to supplement traditional cyber sensors. This information would be fused with process data and provided to the operator so that confidence in the information could be indicated. In addition, randomization of communications traffic and other mechanisms of cyber defense would inhibit an attacker so that recognition and response would prevent the control network compromise and resulting man-in-the-middle attack.

### **3.5 Scenario 5: Safeguards/Nonproliferation**

#### HTGR Area of Applicability: BOP/Fuel Handling System

Current safeguards/nonproliferation sensor designs provide status indications that are displayed independently from the analog (or digital) designs used in commercial reactor and non-reactor nuclear facilities. Detection of sensor tampering has been performed using devices specifically designed to fail-

safe during break-in attempts. In the hypothetical HTGR facility, the state-of-the-art digital control system has a few selected indications of the information retrieved from the safeguards/nonproliferation sensors for display purposes. However, these sensors are remotely transmitted to the safeguards staff so they have easy access to the information over the IP-based network. While the facility is operational, modification and upgrades to the facility are in progress, and a constant flow of external work crews is entering the facility.

During a work day, one of the work crews brings in a laptop to the facility as it is an easy way to reference design information. The worker wants to get internet access during lunch to read the news, so he attaches his laptop to one of the area data ports, trying several until he finds one that works. Port security had not been established for the port he connected to, which is why his connection was allowed. Unbeknownst to him, the laptop has a virus that has turned his system into a bot, allowing a remote hacker to access the network to which the bot laptop is connected. The remote hacker performs a scan of the network through the bot laptop to see what hosts he can find. The traffic between the sensors and safeguards personal are noted, as are the originating and destination hosts. The remote hacker attempts to break into these hosts, and as they use a standard operating system, is able to modify the application that provides the safeguards/nonproliferation data. As calibrations of these sensors are automated on a daily basis, the modification and erroneous data are not recognized until the next calibration cycle. At this time, all movements of fuel are put to a halt while a reconstitution of the special nuclear material records is performed.

Forensic review of the failure in the safeguards/nonproliferation sensors and comparison with video data confirms no direct tampering with the sensors. However, a review of communications records by IT staff identifies the prior, unapproved connection of the worker's laptop. Evaluation of the software application on the sensors finds the modification in the application.

With a resilient control system, safeguards/nonproliferation information is one of the performance areas, along with cyber security, physical security, process stability, and efficiency. Had the movement of the fuel been correlated by independent calculation with process sensors, or even a trend analysis and fusion been used to determine change, this event would have been flagged. Evaluation of the cyber health, fused over this same time period, would have given additional probability for recognition.

### **3.6 Scenario 6: Disruption in Power**

#### **HTGR Area of Applicability: BOP/Power Supply**

The digital control room has two sources of backup power that are separate of the primary power generated by the reactor. Upon failure of the primary power source, the control room draws from external power, and uses an onsite diesel generator as a final backup. The transfer between these power feeds is done via a break-before-make switch, and an Uninterruptible Power Supply (UPS) with battery backup is in place to ensure uninterrupted operation of operator consoles. However, the batteries in these systems require routine maintenance and replacement to ensure individual and lifetime performance. The new digital control system does not receive detailed information on the UPS as it is considered a peripheral and, therefore, will not be able to predict degraded operation.

During an evening shift of the HTGR facility, a regional power surge results in a SCRAM of the reactor, causing a loss of primary power feed to the control room. As external power to the facility is also down, the backup diesel generator kicks on to provide power to the control room. During the transition of the transfer switch, the UPS battery backup fails, and power to the equipment is lost. As a result, all of the computers in the control room reboot. The control room operator knows from experience that the shift supervisor has a display of the information on a computer in her office that operates off of a separate UPS. Confirming its operation with the shift supervisor, another operator on crew is posted at this computer to monitor process status while the computers in the control room reboot.

Evaluation of the situation determines that the batteries in the UPS system supporting the control room had aged and not received normal maintenance due to budget issues. The UPS failure amplified the consequences of the power surge, and lack of state awareness provided no advanced warning of a building problem. These types of issues have a tendency to occur when least desired, because they typically occur under abnormal, non-routine circumstances.

In a resilient control system design, advanced fault diagnosis and detection of all elements that characterize system health are performed, and control changes or warning events are initiated as a result. The UPS is an agent within this design, and while it may have its own fault detection, the control system was not aware of its true health. The resilience of the human was noted in the response to this issue, but was not something either a procedure or control system design was intended to capture. The operator acted out of knowledge. In a resilient design, this ability to embed the operator in responding would have been directly afforded. For example, providing the operator the knowledge that a UPS was failing and indicating flexibility to select more than one source of power to the consoles until the failing UPS was repaired.

### **3.7 Scenario 7: Steam Generator Leaks**

#### HTGR Area of Applicability: HTS

HTGRs have a variety of water sources differing on the type of power conversion system and the operating conditions. The direct steam-Rankine cycle is separated from the primary helium loop by a steam generator. Should steam generator be connected in the primary loop, steam generator failure could lead to water ingress. This is true both at power and during shutdown because of the high enthalpy of the system and the pressure conditions of an HTGR.

During normal operation, steam generator failure could result in steam in the primary system. If the plant is in cold shutdown mode, failure would result in water in the primary system. Since the primary pressure is lower than secondary pressure at power, a steam generator tube break during operation would cause secondary water to migrate to the primary helium loop.

In a resilient control system design, advanced fault diagnosis and detection of all elements that characterize system health are performed, and control changes or warning events are initiated as a result. A resilient design considers the overall efficiency and stability of the coupled processes holistically. While stability is normally a higher-priority interest than efficiency, in this case both were affected. Considering the individual subprocesses as agents working within a global philosophy, the water ingress would be recognized and corrections made to the control parameters to minimize the total impact. In a resilient design, the ability to aid the operator in responding can be directly afforded. For example, providing the operator the knowledge that a leak is occurring and indicating flexibility to select options to minimize effects on the system until the failing component is repaired. Resilient controls can detect leak-before-break and minute leaks as they occur while simultaneously providing the operator this event information with a level of confidence. Resilient design also suggests operator actions or automatic performance of these actions leading to problem correction prior to catastrophic failure. In the event of a large break without prior leak, resilient controls assist in timely and orderly shutdown.

### **3.8 Benefits to HTGRs – Filling the Gap between Resilient and Traditional Controls**

Control Systems and their associated instrumentation must meet availability and resiliency parameters. Reliable and resilient control systems will be necessary for the HTGRs to be enhanced economically and provide increased availability and stability.

While fundamental monitoring and control principles can be applied to achieve a level of success in preventing security events, these techniques are primarily reactive. The basis of resilient design requires consideration of all threats and measures by which proper operation is determined. These measures,



which can be categorized as cyber and physical security, process efficiency and stability, and process compliancy, provide the operating requirements that are monitored for state awareness.

Resilience considers the multiple facets of requirements that drive the performance of control systems in a holistic fashion, whether they are security or stability, stability or efficiency, human interactions, or complex interdependencies. Traditional control philosophies lack the depth to satisfy these requirements, such as graceful degradation of hierarchical control while under cyber attack or the inferred operating parameters in the event of loss of signal. A resilient control system considers these diverse requirements, thereby developing an adaptive capacity to complex events that can lead to failure of traditional control system designs.

The need for a resilient control system is economic and practical, specifically: extending the longevity of the equipment, making operations more efficient, better utilizing existing operators and support staff, increasing stability when coupling with multiple processes, and integrating process measures, such as cyber security and process efficiency.

## **4. TRADITIONAL CONTROL SYSTEMS**

Since the advent of the proportional-integral-derivative feedback loop in the first half of last century, automatic control systems have developed from the original analog to now primarily digital technology. From the 1970s until now, many digital technologies have developed from programmable logic controllers to distributed control systems and supervisory control and data acquisition systems.

Industrial processes designed and built in the 1960s, 70s and early 80s typically employ analog instrumentation with automation to the extent allowed by such systems. With the growth in digital technologies and obsolescence of analog instruments and controls, industrial plant have retrofitted to digital instrumentation either plant-wide or one system at a time. This method of implementation lends itself to employing islands of automation with limited inter-connectivity and limited ability to control complex interactions between systems. The current fleet of LWRs, similar to U.S. industrial plants built during the same period, employ a mix of analog and digital I&C. Safety significant systems use analog instrumentation and balance of plant systems have often been upgraded to digital I&C. Upgrades to digital instrumentation and controls are guided by NRC's Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*,<sup>9</sup> but still lack the integrated benefits gained from a bottoms up design. With HTGRs in the early phases of design, opportunities exist to provide an integrated, holistic approach to plant instruments, controls, and automation.

Control systems may be applied to a variety of industrial processes; be simple or complex; employ analog or digital components; and use manual control or significant automation with nonlinear controls, fuzzy logic, and process optimization. Regardless of application, most control systems perform the same basic functions in a similar flow. This section contains a high-level description of the current traditional control systems commonly implemented in industrial process applications, including the current fleet of LWRs, along with descriptions of common terminology.

### **4.1 Traditional Control System Functional Framework and Definitions**

A control system may be defined as “a device or set of devices to manage, command, direct or regulate the behavior of other devices or systems”<sup>2</sup> or “procedures designed and established to check, record, regulate, supervise, authenticate, and (if necessary) restrict, the access to an asset, resource or system.”<sup>3</sup>

Figure 3 illustrates the functional framework diagram for a traditional control system as implemented in LWRs.

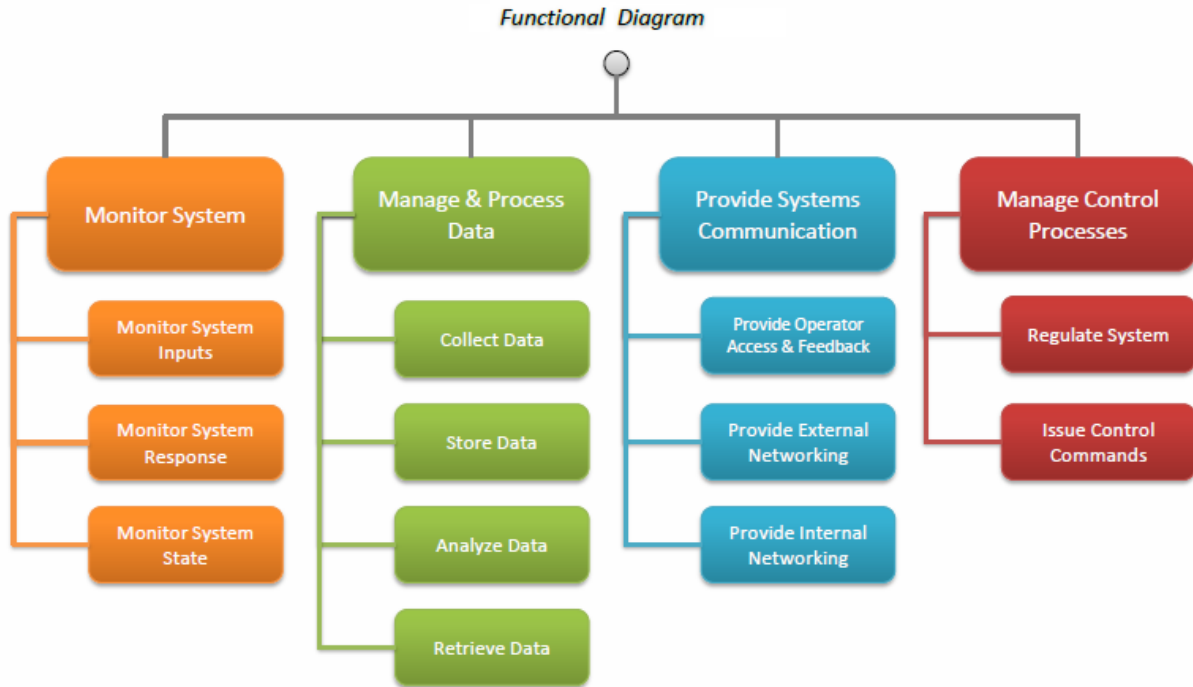


Figure 3. Traditional controls functional framework.

The *Monitor System* high-level function shown in Figure 3 contains the functions and processes for collecting state, input, and response data to measure a controlled system. The *Monitor System Inputs* function monitors instrument readings and observations about the controlled system. The *Monitor System Response* function monitors instrument readings and observations about outputs to the controlled system. The *Monitor System State* function characterizes the system and provides a picture of the system operability in the past or present.

The *Manage and Process Data* high-level function contains the functions and processes for directing the collection, processing, storage, analysis, and retrieval of system data. The *Collect Data* function receives raw analog or digital transmissions from instruments or observational sensors as data. The *Store Data* function refines, formats, or converts raw data suitable for subsequent secure storage available for immediate or future use. The *Retrieve Data* function obtains data from storage for analysis or system/operator use. The *Analyze Data* function performs engineering evaluation of data for purpose of highlighting useful information, suggesting conclusions, or supporting decision making.

The *Provide Systems Communications* high-level function contains the services, systems, and mechanisms that a control system uses to gather or provide information and/or the interaction of these services, systems, or mechanisms with each other. The *Provide Operator Access and Feedback* function enables communications between the control system and a human. The *Provide External Networking* function enables communication between the control system and any external (to the control system) entity. The *Provide Internal Networking* function enables communication within the control system.

The *Manage Control Processes* high-level function contains the control functions for guiding, maintaining, or making changes to the entire controlled system by means of mechanical, optical, or electronic systems. The desired output is achieved by means of issuing control commands and/or regulating the system. The *Regulate System* function analyzes the inputs and state to determine the changes necessary to bring the controlled system into conformity. The *Issue Control Commands* function sends signals to the controlled system.

## 4.2 Traditional Control System Functional and Operational Flow

Most traditional control systems follow a similar flow to accomplish the required functions. One method for depicting this traditional flow is shown in Figure 4. The controlled system provides monitored system inputs to be managed and processed. The system response and system state are also managed and processed to provide operator feedback, provide information to external networks, regulate the system, or issue control commands.

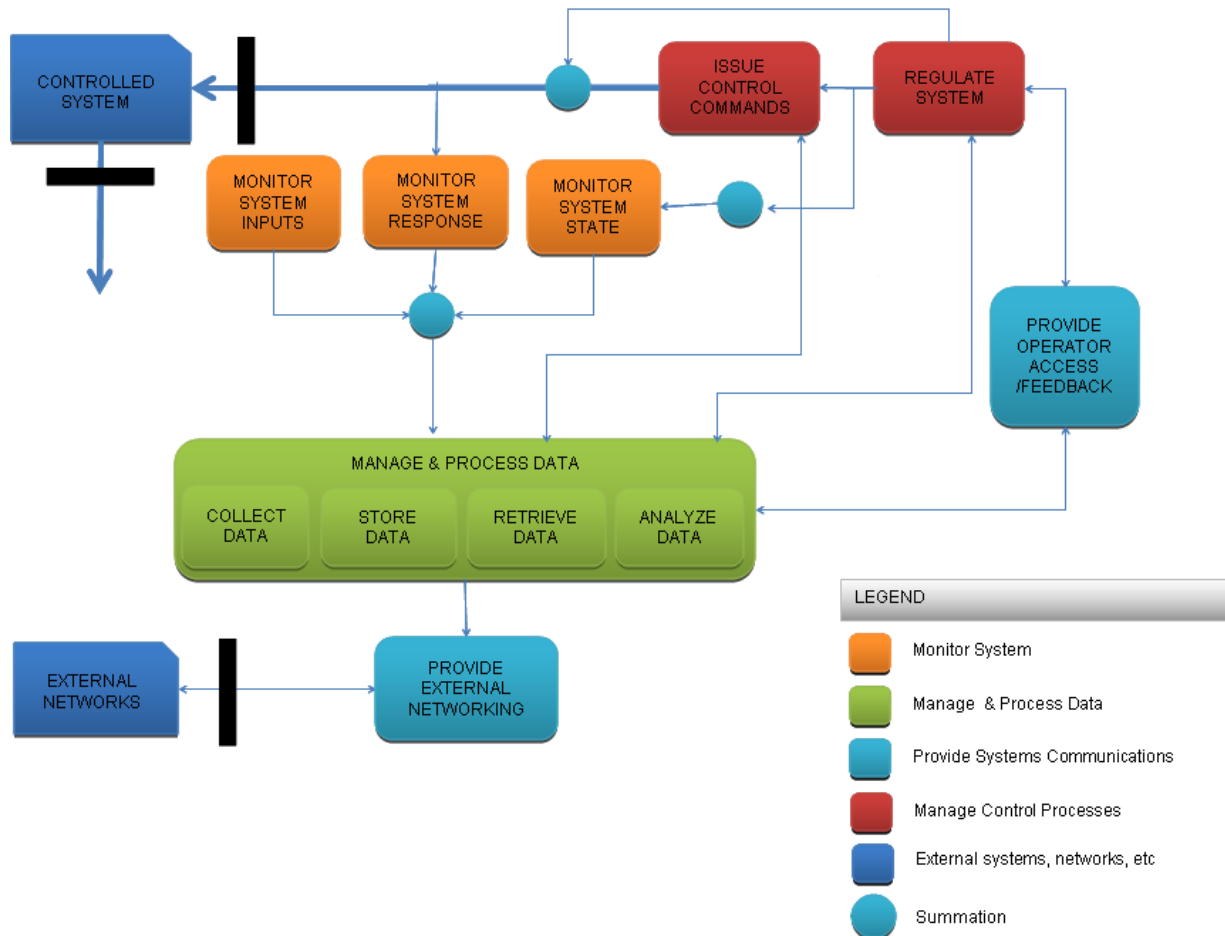


Figure 4. Traditional controls functional flow.

Traditional controls may also be thought of in terms of data collection and control, data processing, and human systems interfacing, as shown in Figure 5. Data collection and control monitors the system status and process sensors. Data processing is very rudimentary in traditional controls and allows for single and limited multi-loop regulatory control. Logic is available for interlocking with alarms settings. The information received from the system status and process sensors is analyzed and provided to a user through a common interface. The user is not usually targeted with the information, but is presented with a large volume of data to sift through. The user may be an operator, engineer, manager, or other person of a need to know status. Through the common interface, the human provides input to the control system to help regulate and provide equipment protection. Control devices implement the updates through redundancy, fault mitigation, and perhaps other processes. Cyber security, nonproliferation sensors, and physical security sensors are in place as bolt-on attachments and are not integrated into the control system design as a holistic process in either traditional controls or new advanced controls currently used in LWRs.



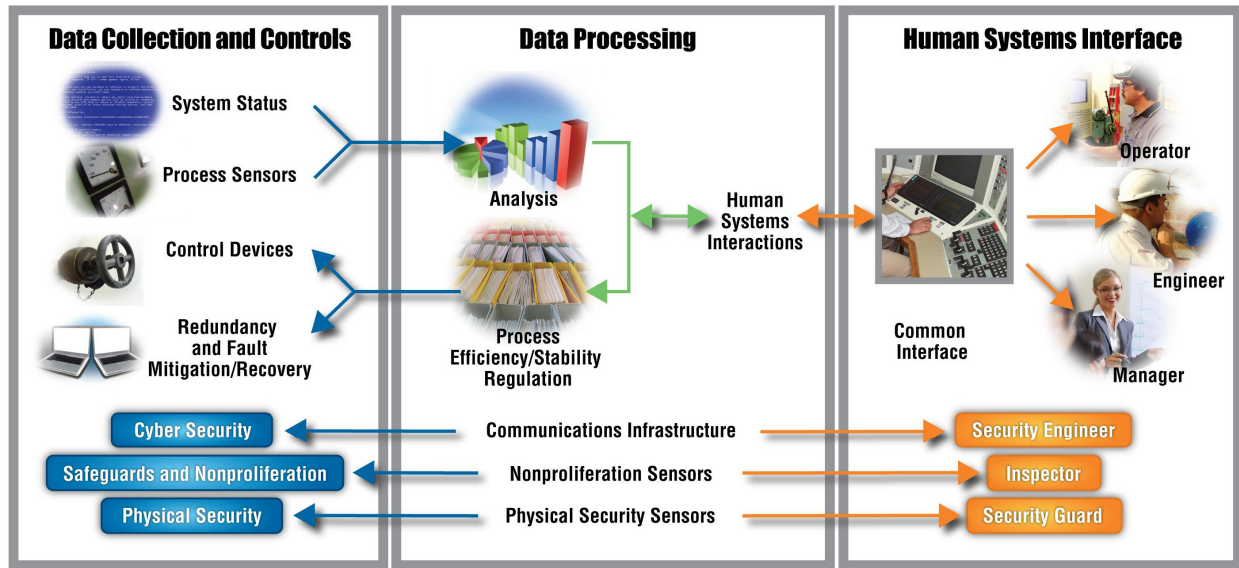


Figure 5. Traditional control system operational flow.

A key feature of traditional control systems is the integration of operations. The operator of a traditional control system can view all necessary information from a single terminal. Traditional control systems are also simpler to implement since large amounts of data exist to provide basis for analysis of systems and many operators have been trained to manage this type of controls.

## 5. RESILIENT CONTROL SYSTEMS

With HTGRs in the early phases of design, opportunities exist to protect the capital investment associated with the key systems of a HTGR by integrating a holistic approach to plant instrumentation, controls, and automation with resilient controls. Resilient control systems necessitate a paradigm shift with respect to the methods historically used in control systems and their design. The move from reactive to proactive control of plants and mechanisms, by which the evaluation and verification of designs is considered all the way from design through implementation stages of resilient control systems, is enabled by this paradigm shift. The key features of resilient controls are state awareness and resilient design. As shown in Figure 6, state awareness provides essential knowledge of operating parameters to fully characterize the decision space. Resilient design provides an adaptive capacity for response to threats, including those that are not well characterized by traditional means. In HTGRs, resilient control systems will be designed, installed, operated, and maintained to survive a natural disaster, human error, or intentional cyber attack with no loss of critical function. This section contains a high-level description of resilient control systems implementation and enhancements to efficient operation in HTGRs, along with common resilience terminology.

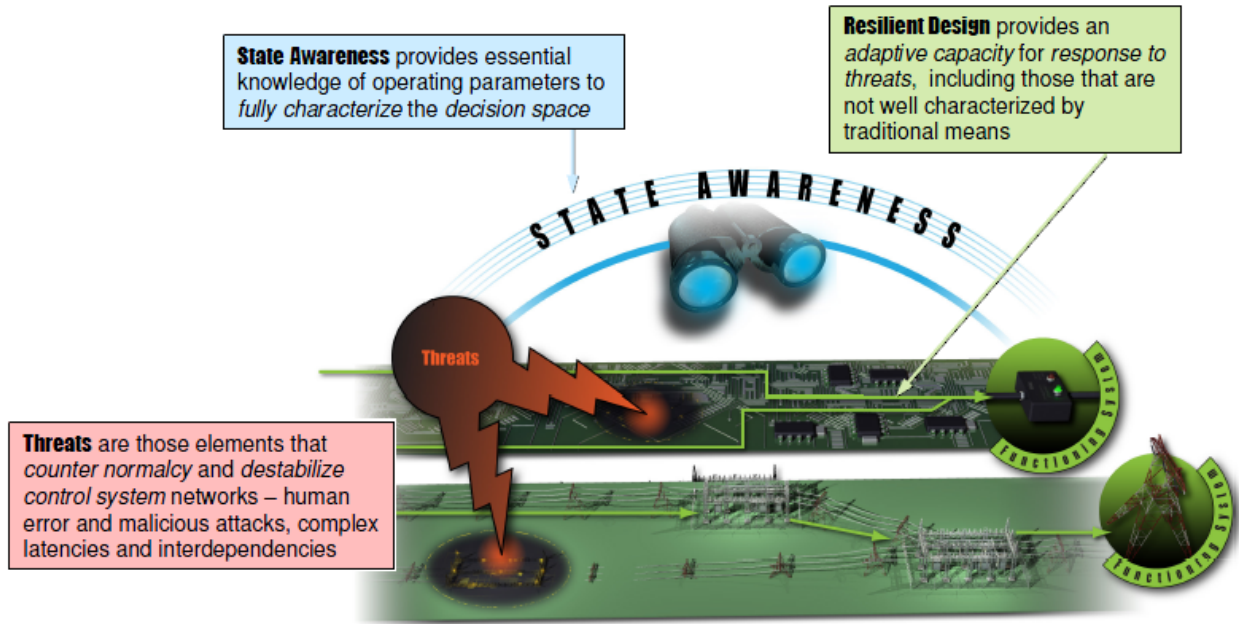
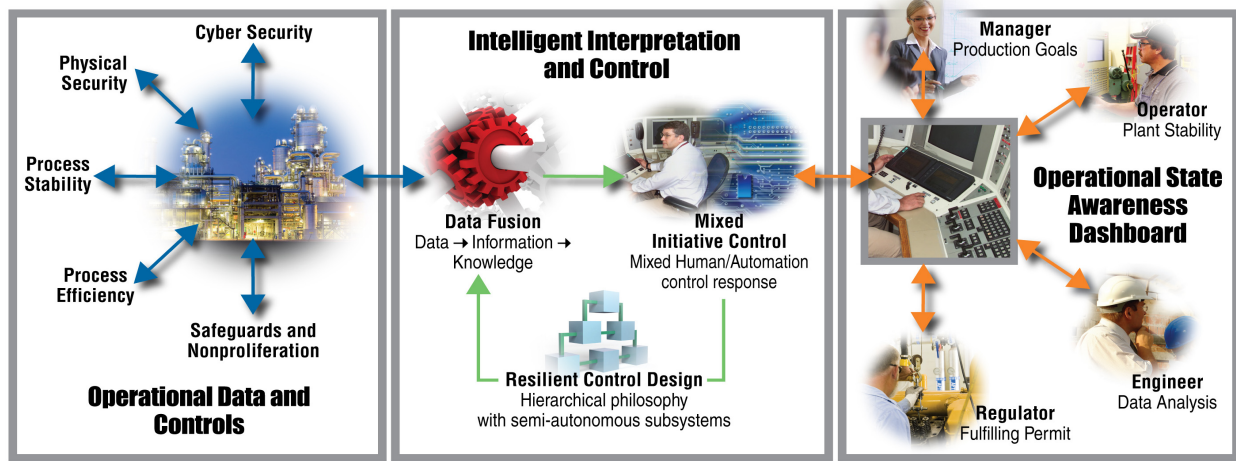


Figure 6. State awareness, resilient design, and threats.

## 5.1 Resilient Control System Functional Framework and Definitions

A resilient control system may be defined as a control system that considers the multiple facets of requirements that drive the performance of control systems in a holistic fashion, whether they are security or stability, stability or efficiency, human interactions, or complex interdependencies. A resilient control system may also be defined as a control system “that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.”<sup>5</sup>

A resilient control system has a similar functional framework to the traditional controls framework, as shown in Figure 3. The differences between the two exist in the depth, capabilities, and philosophical goals of the two types of controls, such as the holistic integration of performance parameters in resilient controls versus the separate, global situational awareness in traditional control systems. As shown in Figure 7, another difference is the consideration of human benefits in resilient control systems versus seeing human error in traditional control systems. These differences are discussed in this section and the impacts upon operational efficiency and protection of capital investment of these differences are discussed in detail in Section 6.



09-50368

Figure 7. Resilient control system.

In addition to the capabilities of traditional control systems discussed in Section 4, a resilient control system framework encompasses the two areas of state awareness and resilient design, as illustrated in Figure 6. State awareness provides the plant operator with a means of understanding the resilience and stability of systems in real time and the extent to which the operator can rely upon the presented information. State awareness protects the capital investment associated with the key systems of a HTGR by ensuring the operator has the necessary information to make correct decisions. Areas of resilience include cyber awareness, human systems, and complex, networked control systems. A notional measure of resilience is in the adaptive capacity or the ability to respond to a threat, remain resilient, and maintain minimum acceptable functionality.

In HTGR, a resilient control system monitors the system, manages and processes data, provides system communications, and manages the control processes in a secure, proactive, and adaptive way. Fundamental monitoring and traditional control principles applied to achieve a level of success in preventing security events are primarily reactive. A goal achieved by resilient controls is to be proactive, rather than reactive, in controlling HTGR plants to increase operational efficiency. The basis of resilient design requires consideration of all threats, all steps required to determine proper operation, and counteractive measures to ensure proper operation. These measures, categorized as cyber and physical security, process efficiency and stability, and process compliancy, provide the operating requirements monitored for state awareness.<sup>2</sup>

### 5.1.1 Monitor System Functional Additions

In addition to the traditional *Monitor System* functions and processes for collecting state, input, and response data to measure a controlled system (see Figure 6), a resilient control system also provide an increased level of cyber and physical security, increased process stability and efficiency, and nonproliferation and safeguards not seen in traditional control systems to protect the capital investment.

Cyber and physical security provides data authentication and diversity to ensure the integrity of cyber and physical environments. It also provides a perspective on the environment and protection from intrusions, some of which could impact the integrity of the control system. Diversity of indicators is needed, especially cyber security, as it is currently not well characterized. Cyber and physical security employs layers of detection fidelity to refine and prioritize discrete targets of interest. In a resilient control system, cyber security, nonproliferation, and safeguards are a holistic part of the system. State awareness is also achieved in a resilience control system by the randomization of system attributes to confound attacks while maintaining determinism for the control application.

Process stability and efficiency predict and diagnose deviations from nominal behavior, migrating the design from reactive to proactive, and need to be analyzed based on global optima. Diagnostics and prognostics are needed to ensure a graceful degradation when the multiple sources of data (signals) fail, which could defeat the benefit of looking at a global optima. The optimization of subsystems to a global maxima or minima, providing a holistic perspective in ensuring plant safety and efficiency, is also a feature of process stability and efficiency. State awareness is also achieved in a resilience control system since process stability and efficiency provide adaptive capacity based on an information quality judgment, overcoming brittleness arising from sensor dependencies. Resilient controls are built upon supervisory control, which considers the dynamic interactions of plant systems and incorporates advanced control theory.

Nonproliferation and safeguards provide timely knowledge of the location and movement of nuclear material within a nuclear facility. Nonproliferation and safeguards of the future will be dependent on a resilient control system for monitoring movement of special nuclear material through a process, and not just on the traditional independent measurements. Advanced techniques, including monitoring and models, will better characterize and control this movement. Real-time knowledge of plant activity prevents downtime of facilities and the diversion or misuse of nuclear material. In a resilient controls system, process accountancy provides enhanced awareness of the nuclear material inventory and status.

Resilient control systems also monitor and anticipate the internal system (such as instrument readings and states of the control system) and global functions of the system. A resilient control system predicts and anticipates abnormal behavior resulting in a proactive design. In resilient controls, the subsystems are globally optimized (autonomy configuration) and future optimization is anticipated resulting in a fluid system that is able to optimize while running. Resilient control systems are capable of predicting and locating the cause of system failures before the fact and then provide signals inferred from system data to relevant entities versus providing only the received signals in traditional control systems. Resilient control systems provide adaptive capacity for degraded signals (improve signal quality) based on information quality judgment, thus overcoming brittleness arising from sensor dependencies.

### **5.1.2 Manage and Process Data Functional Additions**

In addition to the traditional system *Manage Process Data* functions, resilient control systems also consider human and automation for methodologies and algorithms. Resilient control systems integrate diverse indicators to increase data confidence. A resilient control system updates and refines the future system environment model to aid in predicting future events. Resilient controls prioritize information by reducing data to the necessary information, identifying event causes, and improving system characterization, as shown in Figure 8. Resilient design, a key feature of a resilient control system, goes beyond being just reliable by many techniques including data fusion, mixed initiative, control system, state dashboard, and human system. Resilient controls have the ability to anticipate as well and predict and diagnose abnormal behavior. Data fusion aids a resilient design by numerous methods, including the following:

When managing and processing data, resilient controls can fuse diverse process data to proactively recognize threats within each measure of normalcy and prioritize response. Resilient controls consider both human input and automation to determine algorithms and methodologies, as well as integrate diverse indicators, such as cyber security and process data, to determine the desired operation. Resilient controls also prioritize the information provided to the consumer to aid recognition and action. Resilient controls also reduce the data to provide only that information necessary to the operator to achieve the appropriate response. Resilient controls can validate and invalidate of causes for events, e.g., a process upset caused by a failed valve and not cyber attack.

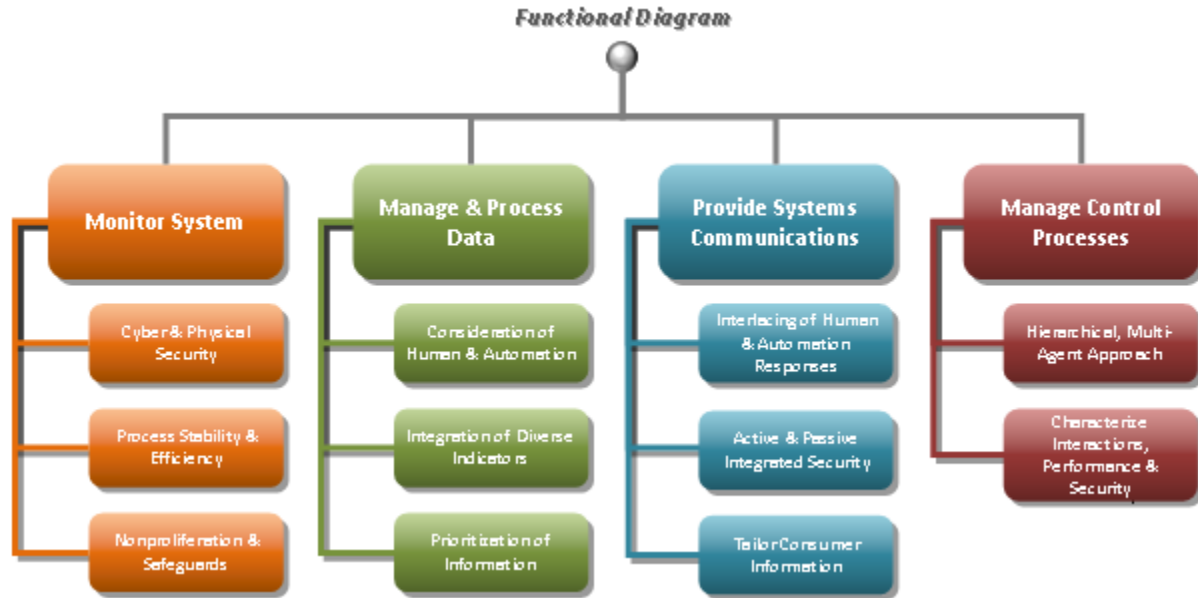


Figure 8. Functional additions of resilient control systems.

### 5.1.3 Provide Systems Communications Functional Additions

Along with the *Provide Systems Communications* functions and processes found in traditional controls, mechanisms in resilient controls integrate automation and human response, provide active and passive security in an optimized manner, and tailor consumer information. HTGRs benefit from the inherent resilience of mixed initiatives in resilient controls in both by interlacing human and automation responses for optimal reaction and measuring and adapting to the user based on current understanding, performance, and the changing environment. Resilient controls maximize the resilience of a reproducible response with reaction to unique situations. Resilient controls employs measurement and adaptation based on current understanding, performance, and changing environment. Threats are adaptively detected and data is authenticated to ensure cyber and physical environments are safe and secure. A resilient control system has randomized system attributes to confound attacks while maintaining determinism for the control application.

Resilient controls integrate active and passive security measures. In a resilient control system, cyber security, nonproliferation, and safeguards are a holistic part of the system. For example, cyber security for data collection and control and advanced cyber security are holistically integrated into multiple levels of data fusion and communications along with the human systems interface reporting. A resilient control system is able to identify and distinguish between normal and abnormal communications. In a resilient control system, threats are adaptively detected and data is authenticated to ensure cyber and physical environments are safe and secure. Resilient controls have an atypical architectural design to take away the adversarial advantage while, at the same time, changing the system attributes to appear random in response and characteristics.

Targeting the consumer of the information, resilient controls tailor what is presented and how interactions between the human and the interface form the basis for proper or improper judgments. A resilient control system authorizes interaction level by individual certifications, responsibilities, and measured performance. Resilient controls also present the information in reflection of the needs of the consumer (whether operator, manager or engineer) and his or her respective responsibilities. A resilient control system provides user adapted information access and feedback, which utilizes a user interface screen and information adapted to the individual user. A resilient system facilitates joint human and automation cognitive decision making for optimal reaction.



Resilient controls provide advanced cyber security integration into multiple levels of data fusion and communication and report to the human systems interface. A resilient control system is able to identify and distinguish between normal and abnormal communications and ensure the integrity of the cyber and physical environment by adaptively detecting threat and authenticating data. Resilient controls provide layers of detection and network security responses to refine and prioritize discrete targets of interest. Resilient controls provide randomized system attributes to confound attacks while maintaining determinism for the control application and provide user-adapted information access and feedback. Interlaced human and automation cognitive decision making is also facilitated by resilient controls for optimal reaction. Resilient control systems allow the user to configure autonomy and tailor the information to the consumer receiving it. Measurement and adaptation is provided to the user based on the current understanding, performance, and changing environment in resilient control systems.

#### **5.1.4 Manage Control Processes Functional Additions**

In addition to the *Manage Control Processes* functions performed by traditional controls, resilient controls employ a hierarchical, multi-agent approach to supervisory design and characterize interactions, performance, and security to provide graceful degradation of autonomous actions and utilize signal inference upon loss of sensory capacity.

Resilient controls enlist a hierarchical, multi-agent approach to supervisory design that considers the control system and affected operation holistically. A hierarchical control system design provides a robust and adaptive mechanism for optimizing control system performance to measures of normalcy. A hierarchical, multi-agent approach also provides a global perspective to complex system design, which can be delegated appropriately to lower echelons along with a predefined level of control autonomy. The resulting control system design provides a non-fragile mechanism for optimizing control system performance. To provide faster responses, feedback and response in a resilient control system occur close to the point of interaction with the application.

Resilient controls characterize interactions, performance, and security to provide graceful degradation of autonomous interaction based upon loss of sensory capacity. In a resilient control system, the ability to characterize interactions, performance, and security becomes more critical to ensuring resilience.

Resilient controls distribute system resources and execute internal operations in real time to allow users to locate and maintain awareness of materials and resources. Resilient controls proactively model the future control system and its environment. Resilient controls employ a hierarchical, multi-agent approach to supervisory design that considers the control system and affected operation holistically. Independent oversight outside of the echelon ensures state awareness is accurately communicated up and philosophy is communicated down in resilient controls.

### **5.2 Resilient Control Functional and Operational Flow**

One method for depicting the traditional functional flow is described in Section 4.2. To enhance the efficient operation of key systems, a resilient control system usually follows this traditional functional flow while implementing the key functions of resilient controls in addition to the functions of traditional controls. Similar to those in traditional control systems, resilient control system inputs and the system's response and state are managed and processed to provide operator feedback and information to external networks, regulate the system, or issue control commands.

While a resilient control system follows a similar operational flow to a traditional control system, there are many differences the state awareness level, the implementation level of resilient design, and in how threats are addressed. These differences provide a significant delta in the operational normalcy of the system.

Unlike traditional control systems, resilient control systems are designed, installed, operated, and maintained to survive a natural disaster, human error, or intentional cyber attack with no loss of critical

function. This enhancement of efficient operation is no small challenge in a sector that is complex, highly networked, and sensitive to the mildest failure. To protect the capital investment associated with HTGR, research is required to achieve resilience, address the threats in next generation control systems, and integrate an understanding of cyber security, human interaction, and complex network design. The integration of these three aspects are introduced in the concepts of data fusion, mixed initiative, and hierarchical control system design, as shown in Figure 9.

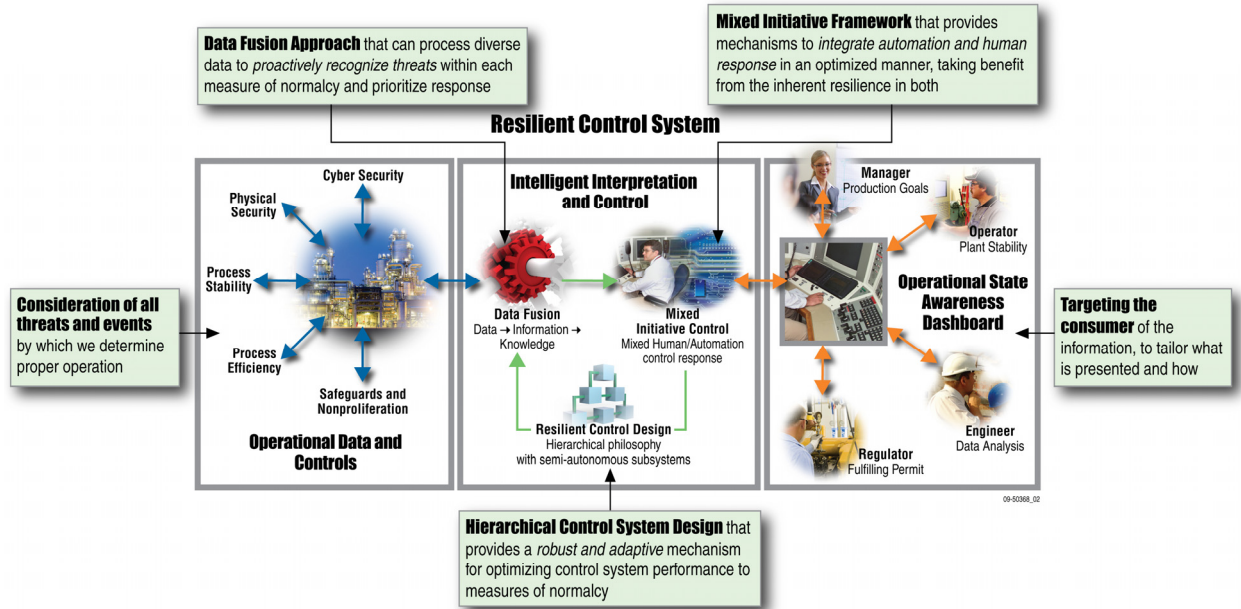


Figure 9. Resilient control system operational flow.

Data fusion plays a significant role in tailoring information to the user and provides a broader state awareness for items such as malicious cyber attack. Data fusion technology can also integrate diverse forms of data, allowing contrast or variations from normalcy to be recognized. With highly integrated combinations of multiple control systems, data fusion research is needed to quickly recognize human error or malicious cyber attack and prevent a negative impact cascading to multiple process systems. A data fusion approach can process diverse data to proactively recognize threats within each measure of normalcy and prioritize responses.

Mixed initiative control provides an optimized combination of automation and human response to achieve the most resilient reaction from both for increased efficiency. Humans can be more effective at recalibrating response to changing environments, but must be effectively modeled to ensure the proper integration with automation. The mixed initiative framework is proposed to provide mechanisms to integrate automation and human response in an optimized manner, taking benefit from the inherent resilience in both.

When considering the integrated operation of varied processes with competing objectives, a hierarchical, multi-agent approach to control system design lends resilience and ensures the required overall performance is maintained according to the measures by which normalcy is accessed (as it considers the integrated operation holistically). A hierarchical, multi-agent approach also provides a global perspective to complex system design, which can be delegated appropriately to lower echelons along with a predefined level of control autonomy. The resulting control system design provides a non-fragile mechanism for optimizing control system performance and protection of capital investment.

## 6. HTGR APPLICABLE FUNCTIONAL GAP ANALYSIS

Traditional LWR control and safety related reactor protection systems have extensive and thoroughly vetted requirements. Implementing a resilient strategy above and beyond the existing traditional systems does not negate or challenge any of those existing requirements. A resilient strategy seeks to improve availability and enhance the economic competitiveness of the plant.

This section identifies existing gaps between a traditional LWR control system and a resilient control system, as applied to HTGRs, and presents several of the many benefits of moving from traditional controls to resilient controls. To identify the gaps, traditional control systems and resilient control systems both underwent functional analysis. This analysis highlighted differences in the measures of normalcy, data fusion, resilient control design, mixed initiative control, and adaptive capacity for each item in the controls functional framework. The gap analysis process is shown in Figure 10.

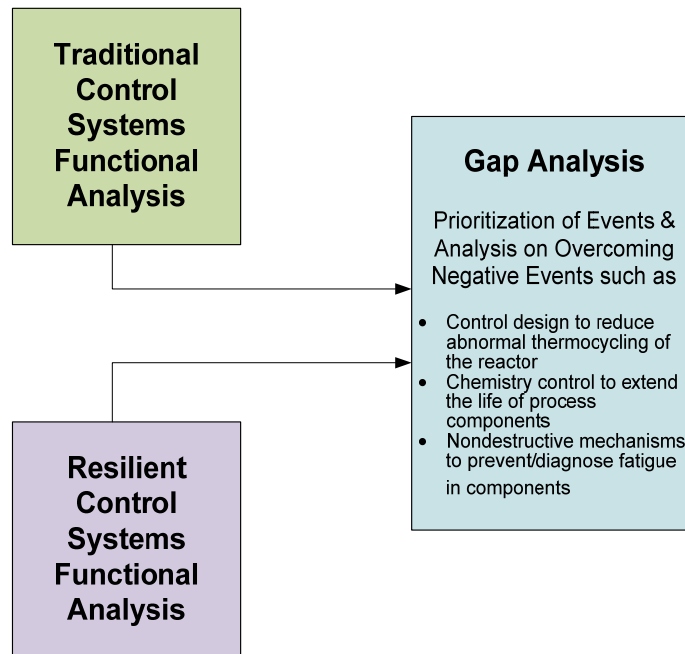


Figure 10. Gap analysis process.

### 6.1 Monitor System Gap Analysis

The additional functions required to move from a traditional LWR to a resilient control system in performing the *Monitor System* function are numerous for a HTGR. When monitoring the system, resilient controls consider all threats and events by which proper operation is determined. Features not included in traditional control systems include holistically integrated cyber and physical security, process stability and efficiency, and nonproliferation and safeguards as shown in Figure 11. The functions performed by a traditional control system are shown in dark orange while the additional high level functions performed by a resilient control system is shown in light orange.

Cyber and physical security provides data authentication and diversity to ensure the integrity of cyber and physical environments. It also provides a perspective on the environment and protection from intrusions, some of which could impact the integrity of the control system. Diversity of indicators is needed, especially cyber security, as it is currently not well characterized. Cyber and physical security employs layers of detection fidelity to refine and prioritize discrete targets of interest. In a traditional control system, cyber security is a separate entity, as is the security engineer; hence, a traditional control



system does not have access to cyber security, physical security, and nonproliferation monitoring. Degradation that affects control system integrity, lack of a common interface, prioritization of responses, and other benefits of having the additional information in one location are also not recognized. In a resilient control system, cyber security, nonproliferation, and safeguards are a holistic part of the system.

Process stability and efficiency predict and diagnose deviations from nominal behavior, migrating the design from reactive to proactive, and need to be analyzed based on a global optima, as traditional control systems assume efficiency and stability based solely upon stabilization of subsystems. Diagnostics and prognostics are needed to ensure a graceful degradation when the multiple sources of data (signals) fail, which could defeat the benefit of looking at a global optima. The optimization of subsystems to a global maxima or minima, providing a holistic perspective in ensuring plant safety and efficiency, is also a feature of process stability and efficiency.

Nonproliferation and safeguards provide timely knowledge of the location and movement of nuclear material within a nuclear facility. Nonproliferation and safeguards of the future will be dependent on a resilient control system for monitoring movement of special nuclear material through a process, and not just on the traditional independent measurements. Advanced techniques, including monitoring and models, will better characterize and control this movement. Real-time knowledge of plant activity prevents downtime of facilities and the diversion or misuse of nuclear material.

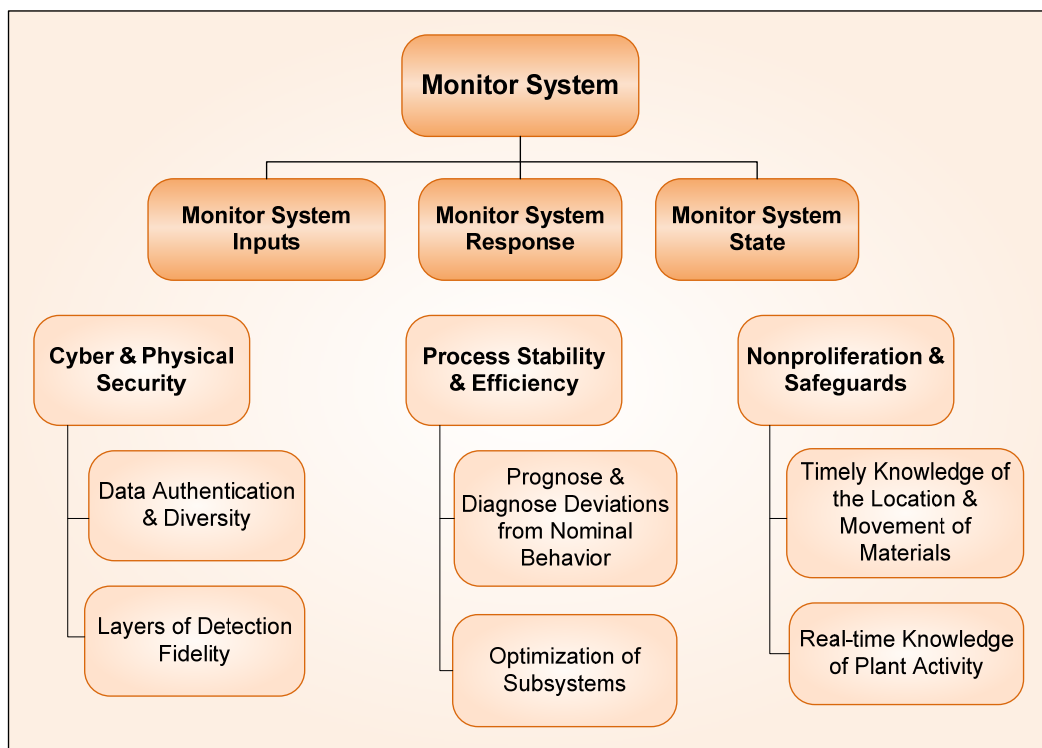


Figure 11. Monitor System with Resilient Features.

In addition to the functions performed by a traditional control system, a resilient control system also monitors and anticipates internal systems (such as instrument readings and states of the control system), and global functions of the system. Resilient controls predict and anticipate abnormal behavior resulting in a proactive and predictive design. They also employ online condition monitoring, which looks at data and diagnoses abnormal behavior through a multitude of different analysis techniques. Once the behavior has been characterized, resilient controls predict failure, maintenance needs, or control to prevent behaviors. Traditional control systems are usually design subsystems optimized for cost, component placement, and longevity. In traditional controls, fixed optimization is created during the design phase. In

resilient controls, the subsystems are globally optimized (autonomy configuration) and future optimization is anticipated, resulting in a fluid system able to optimize while running.

Traditional controls detect and locate the cause of system failures after the fact. Resilient control systems are capable of predicting and locating the cause of system failures before the fact. Resilient control systems also provide signals inferred from system data to relevant entities verses providing only the signals received in traditional control systems. Traditional control systems detect degraded signals (Signal Quality "as is") but are unable to improve them. Resilient control systems provide adaptive capacity for degraded signals (Improve Signal Quality) based on information quality judgment, thus overcoming brittleness arising from sensor dependencies.

## 6.2 Manage and Process Data Gap Analysis

The additional functions required to move from a traditional LWR to a resilient control system in a HTGR performing the *Manage and Process Data* function are numerous. In addition to the functions performed by a traditional control system, a resilient control system considers human and automation aspects in determining algorithms, integrates diverse indicators, and prioritizes information, as shown in Figure 12. The functions performed by a traditional control system are shown in dark green while the additional high-level functions performed by a resilient control system are shown in light green.

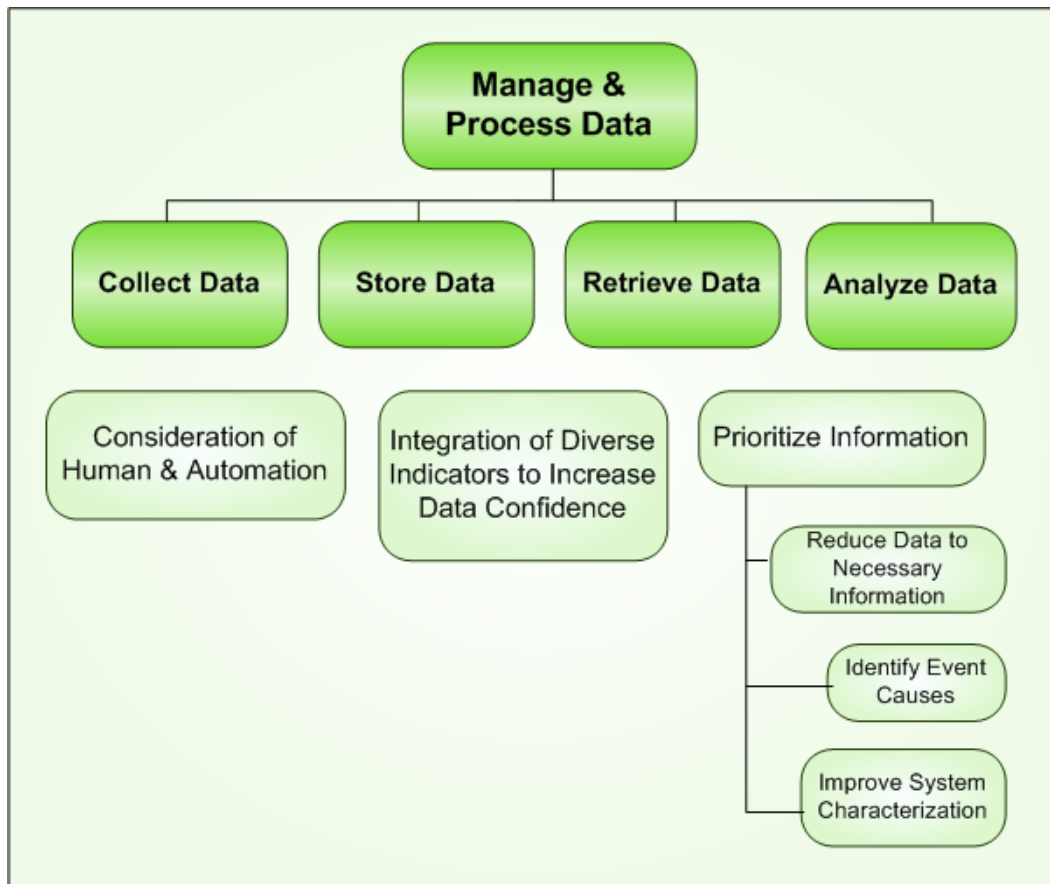


Figure 12. Manage and Process Data with Resilient Features.

A traditional control system directly receives and interprets indicator signals from raw analog or digital transmissions from instruments or observational sensors. Resilient control systems integrate diverse indicators to increase data confidence. A traditional control system operates from a fixed, static model of the system created in the past; conversely, a resilient control system updates and refines the

future system environment model to aid in predicting future events. In addition to collecting, storing, retrieving, and analyzing information the way a traditional control systems does, a resilient control system prioritizes information by reducing the data to the necessary information, identifying event causes, and improving system characterization.

When managing and processing data, resilient controls can fuse diverse process data to proactively recognize threats within each measure of normalcy and prioritize response. Resilient controls consider both human input and automation to determine algorithms and methodologies, as well as integrate diverse indicators, such as cyber security and process data, to determine the desired operation. Resilient controls also prioritize the information provided to the consumer to aid recognition and action.

### 6.3 Provide Systems Communication Gap Analysis

The additional functions required to move from a traditional LWR control system to a resilient HTGR control system in performing the *Provide Systems Communications* function are abundant. The additional functions performed by resilient controls include providing the operator access and feedback, and providing external and internal networking, as shown in Figure 13. The functions performed by a traditional control system are shown in dark blue while the additional high-level functions performed by a resilient control system are shown in light blue.

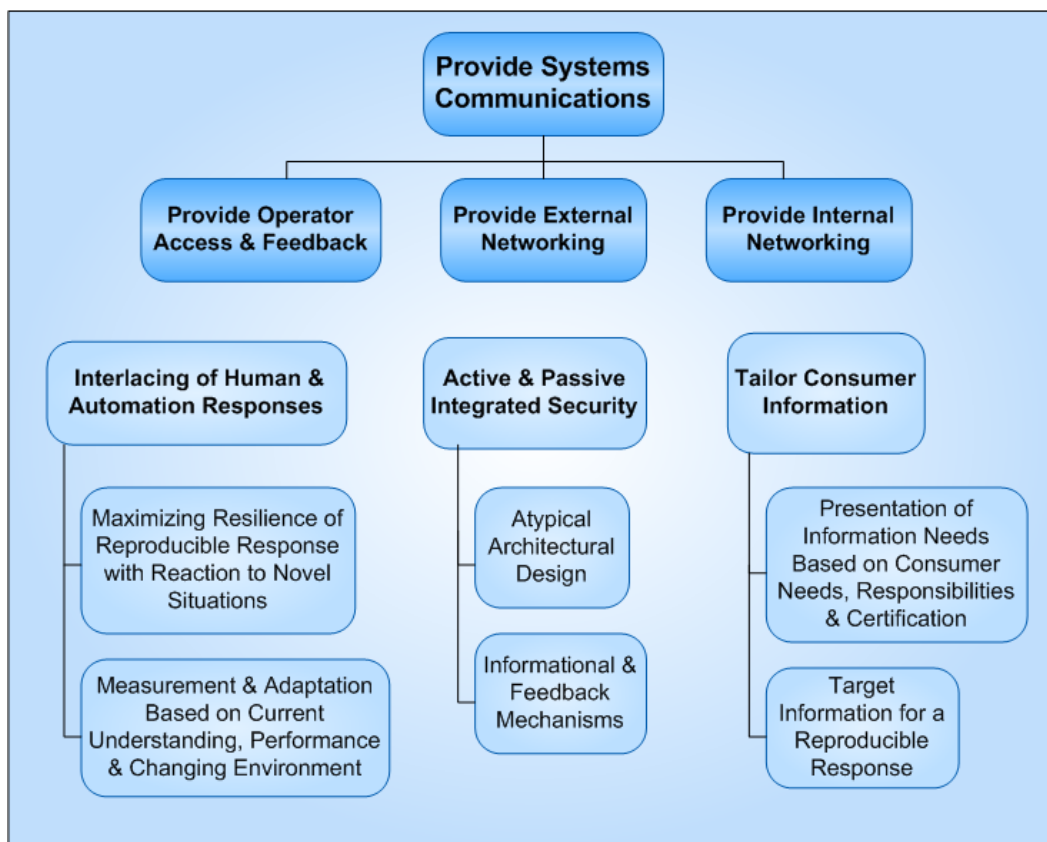


Figure 13. Provide Systems Communications with Resilient Features.

When providing systems communications, mechanisms in resilient controls integrate automation and human response in an optimized manner, benefiting from the inherent resilience in both by interlacing human and automation responses for optimal reaction and measuring and adapting to the user based on current understanding, performance, and the changing environment. Resilient controls maximize the resilience of a reproducible response with reaction to unique situations. In a resilient control system, the

goal is to target information to achieve a reproducible response for the benevolent employee while befuddling the intelligent adversary attacker. Informational mechanisms are in place to understand system health, and feedback mechanisms are used to tie a sensed attack to a corresponding control system change. Methods to model the variability of both the objective and motives of the intellectual adversary and provide a basis for feedback are a part of resilient controls. Resilient controls employs measurement and adaptation based on current understanding, performance, and changing environment. A traditional control system assumes data is authentic and responds to threats after they are identified. In a resilient control system, threats are adaptively detected and data is authenticated to ensure cyber and physical environments are safe and secure. A traditional control system has preset responses to a preset list of threats, whereas a resilient control system has layers of detection fidelity to refine and prioritize discrete targets of interest. A traditional control system has preset and unchanging system parameters, whereas a resilient control system has randomized system attributes to confound attacks while maintaining determinism for the control application.

Resilient control integrates active and passive security measures. In a traditional control system, cyber security is a separate entity, as is the security engineer; hence, a traditional control system does not have access to cyber security, physical security, and nonproliferation monitoring. Degradation that affects control system integrity, lack of a common interface, prioritization of responses, and other benefits of having the additional information in one location are also not recognized. In a resilient control system, cyber security, nonproliferation, and safeguards are a holistic part of the system. For example, cyber security for data collection and control and advanced cyber security are holistically integrated into multiple levels of data fusion and communications along with the human systems interface reporting. In a traditional control system, communications continue as is and are assumed normal. A resilient control system is able to identify and distinguish between normal and abnormal communications. A traditional control system assumes data is authentic and responds to threats after they are identified. In a resilient control system, threats are adaptively detected and data is authenticated to ensure cyber and physical environments are safe and secure. A traditional control system has preset responses to a preset list of threats, whereas a resilient control system has layers of detection fidelity to refine and prioritize discrete targets of interest. Resilient controls have an atypical architectural design to take away the adversarial advantage while, at the same time, changing the system attributes to appear random in response and characteristics. A traditional control system has preset and unchanging system parameters, whereas a resilient control system has randomized system attributes to confound attacks while maintaining determinism for the control application.

Targeting the consumer of the information, resilient controls tailor what is presented and how interactions between the human and the interface form the basis for proper or improper judgments. A resilient control system authorizes interaction level by individual certifications, responsibilities, and measured performance. Resilient controls also present the information in reflection of the needs of the consumer (whether operator, manager or engineer) and his or her respective responsibilities. A traditional control system has a universal maintenance screen interface, which utilizes the same interface screen for any user. A resilient control system provides user adapted information access and feedback, which utilizes a user interface screen and information adapted to the individual user. In a traditional control system, either the operator or automatic response system makes the decision, not both. A resilient system facilitates joint human and automation cognitive decision making for optimal reaction.

## **6.4 Manage Control Processes Gap Analysis**

The additional functions required to move from a traditional LWR control system to a resilient HTGR control system in performing the *Manage Control Processes* function are numerous. When managing control processes, a resilient control system provides additional features in the following areas, as shown in Figure 14:

- Hierarchical, multi-agent approach to supervisory design that considers the control system and affected operation holistically
- Characterize interactions, performance, and security to provide graceful degradation of autonomous interaction based upon loss of sensory capacity

The functions performed by a traditional control system are shown in dark red while the additional high-level functions performed by a resilient control system are shown in light red.

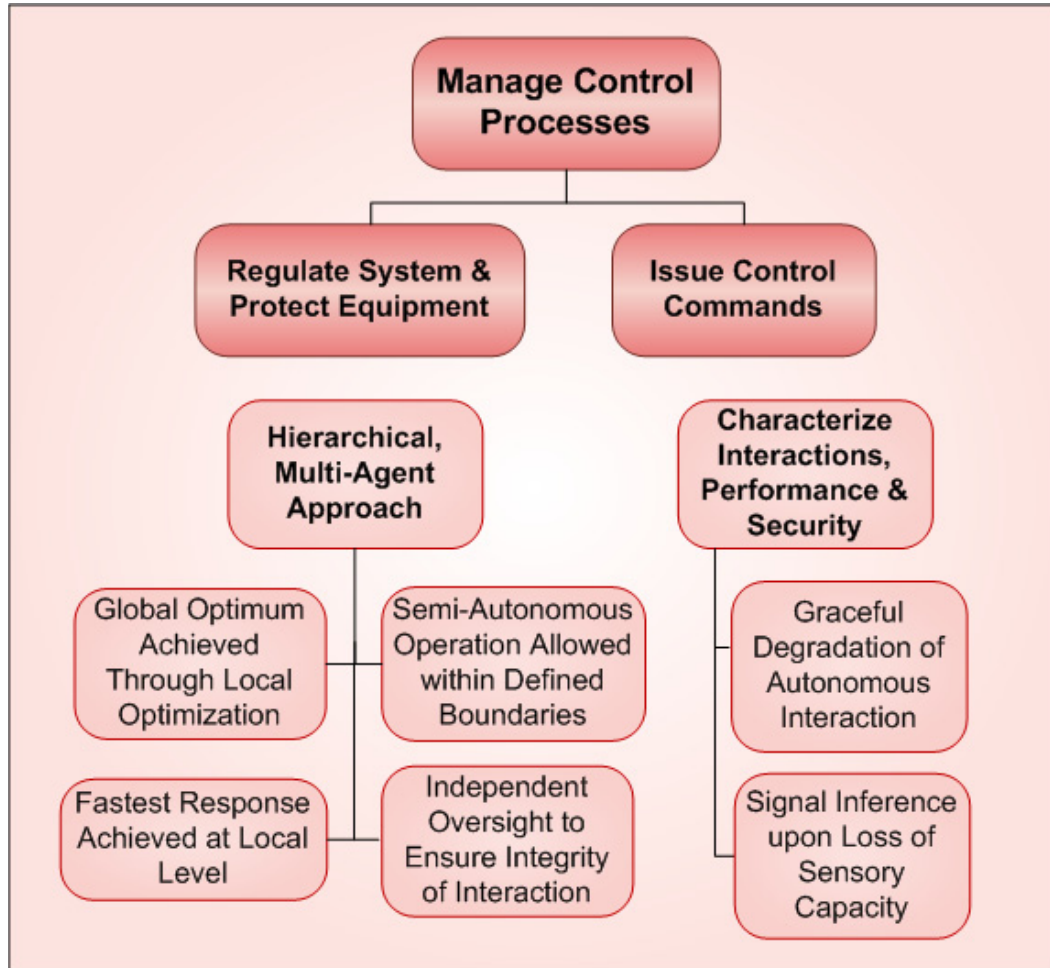


Figure 14. Manage Control Processes with Resilient Features.

Resilient controls employ a hierarchical, multi-agent approach to supervisory design that considers the control system and affected operation holistically. A hierarchical control system design provides a robust and adaptive mechanism for optimizing control system performance to measures of normalcy. A hierarchical, multi-agent approach also provides a global perspective to complex system design, which can be delegated appropriately to lower echelons along with a predefined level of control autonomy. The resulting control system design provides a non-fragile mechanism for optimizing control system performance. Semiautonomous operation is allowed within defined boundaries for lower echelons in resilient control systems. Independent oversight outside of the echelon ensures state awareness is accurately communicated up and philosophy is communicated down in resilient controls. In a resilient control system, the ability to characterize interactions, performance, and security becomes more critical to ensuring resilience. To provide faster responses, feedback and response in a resilient control system occur close to the point of interaction with the application.



In a traditional control system, a reactive model of the current system and environment may exist, whereas a resilient control system proactively and continuously models the future system and its environment. A traditional control system employs a universal human interface, which is the same for all users, and the human system interactions (with no automation) are the common interface. Human system interactions in resilient control systems interlace human and automation responses for mixed initiative control. Mixed initiative control provides a customized interface screen for users and mixes humans and automation for optimal reaction, including the use of human sensors and human correlation. A traditional control system coordinates system functions based on static, preprogrammed information with preset, unchanging functions based on assumptions. A resilient control system validates and prioritizes task execution and regulation responses based on the load, history, current system understanding, performance, and changing environment. In a traditional system the user receives information after the fact, whereas in a resilient system, user measurement and adaptation data is provided in the form of inferred signals so the user has greater insight into the current system and the future system. Supervisory control with redundant signals, which is reactive and after the fact, is utilized in a traditional control system. A resilient system has signals that are integrated, predicted, and inferred to globally optimize the system and provide a future and predictive control environment. Resilient control systems also include mechanisms of graceful degradation while traditional supervisory control mechanisms do not. True global optimization coupled with local interaction ensures a global minima and an acceptable response time.

## **7. STRATEGIC PATH FORWARD TO FILL THE GAP**

This section outlines the necessary steps to fill the gaps and identify research needs between the traditional control systems currently implemented in LWRs and the resilient control systems needed for future HTGRs beyond first of a kind (FOAK). Maturation of the research needs should parallel NGNP development and will be available to benefit future generations of HTGRs. The rating system used to identify the most pressing needs in resilient control research as applicable to HTGRs is discussed in this section along with a few highlights of the current resilient control research underway at the Idaho National Laboratory (INL). Figure 15 illustrates the resilient control system path forward for this document.

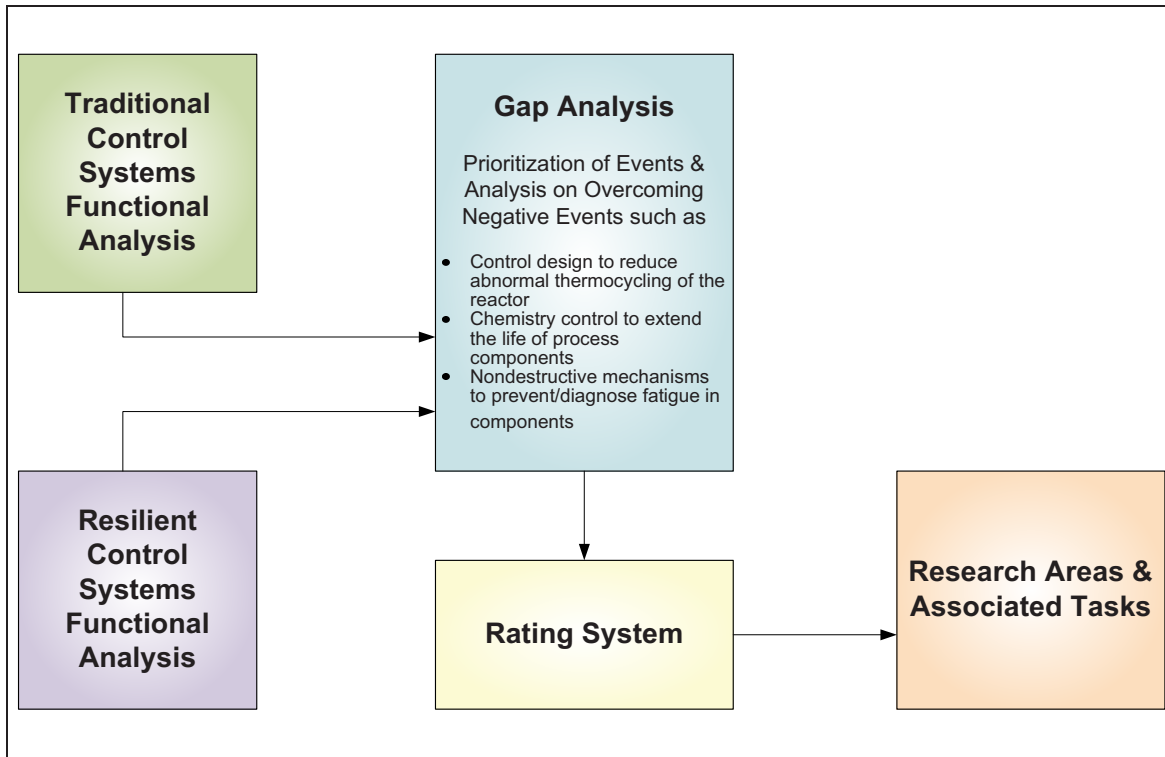


Figure 15. Resilient Control System Path Forward.

## 7.1 Gaps and Research Needs

The highest risks within HTGRs are those risks which, if realized, result in early failure of the key systems and components within the five HTGR plant areas. Table 2 identifies the key systems and components and resilient controls research area that will assist in reducing the risk of early system failure while protecting the investment.

Table 2. Key Systems, Components, and Resilient Controls Research Areas

HTGR Area/Systems or Component	Event	Failure Mechanism	Plant Impact	Resilient Research Area
NHS/RPV HTS/IHX, X-Vessel PCS/Steam Generator	Undetected change Lack of awareness of plant condition	Failed or Drifted Sensor	Plant shutdown Additional thermal cycling Early vessel failure	Process stability and efficiency (Signal inference) Tailor consumer information (data fusion)
PCS/ SG	Superheat or phase boundary occurs at metal weld	Corrosion Fouling	Premature tube rupture Equipment replacement Plant shutdown Thermal cycling	Integration of diverse indicators Tailor consumer information

HTGR Area/Systems or Component	Event	Failure Mechanism	Plant Impact	Resilient Research Area
NHS, HTS, PCS	End-user induced transients	Complex interactions thermal cycling	Premature equipment failure Plant shutdown Reduced capacity factor	Process stability and efficiency
BOP/I&C	Cyber attack	Intrusion Data compromise	Compromised I&C	Cyber and physical security
BOP/Fuel Handling System	Safeguards and nonproliferation	Safeguards Data compromise	Plant shutdown Increased thermal cycling	Nonproliferation and safeguards
BOP/Power System	Inadequately designed backup power	Equipment malfunction	Equipment shutdown, Plant shutdown Increased thermal cycling	Consideration of Human and Automation
PCS	Steam generator leaks	Tube rupture	Water ingress into primary system Reduced power factor Reduced equipment life	Interlacing of human and automation Integration of diverse indicators

## 7.2 Method of Identifying Most Pressing Needs

The method used to identify and rate the most pressing resilient control system needs builds off of work completed for the NGNP Risk Management System and documented in the *NGNP Risk Management Plan*.<sup>7</sup> The plan defines risk to the successful operation of the NGNP as the consequence of realizing the event multiplied by the probability of the event occurring, where an event is an accident condition or an adverse scenario that resilient features are intended to mitigate. The resilient control system features become mitigation strategies for reducing risk by lessening the consequence or decreasing the probability of an event or adverse scenario, such as cyber attacks, natural disasters, and human errors.

### 7.2.1 Risk Reduction

In the rating of resilient features for potential resilient control systems, we consider the risk to the project that the resilient features are intended to mitigate. Since risk is the probability of the event occurring multiplied by the consequence that results should the event occur (see EQN1), reducing either probability or consequence serves to mitigate the project risk.

$$\text{Risk} = \text{Probability} \times \text{Consequence} \quad [\text{EQN } 1]$$

Since not all consequences are equal, it stands to reason that the importance of any resilient feature will be determined by its ability to mitigate the consequence and thereby reduce the risk of NGNP unavailability and overall reduction in plant power factor. Likewise, decreased probability reduces risk, and resilient features that reduce probability should be rated appropriately.

For example, cyber attack resulting in system intrusion and reduced data confidence is an adverse scenario with potentially severe consequence. Resilient features, such as Trend Analysis through



randomization, are designed to lessen the consequence through early detection and increased state awareness. Another resilient feature, such as a robust firewall, will lessen the probability of a cyber attack and thereby mitigate the risk. These features allow for the monitoring system to more accurately estimate the current state of a given system parameter with higher consistency and provide the operator with increased state awareness.

Thus, a given resilient feature, if it helps to mitigate the risk, must do one of two things: reduce the probability of the event, or reduce the severity of the consequence upon occurrence. Either of these two effects will reduce risk. We could then assign a rating to the resilient feature in proportion to the amount of risk reduced for each of the events or adverse scenarios evaluated.

Collections of features could have a combined ability to reduce the probability and severity of the consequence of events in a synergistic way and perhaps more so than any of the features could individually. Hence, a rating system should not only rate individual features but also recognizes the benefits of collections of features. Thus, resilient features should be rated on their ability to mitigate risk (i.e., reduce consequence and/or probability of occurrence) and on their ability to increase the potential system resilience as a collection of resilient features.

### 7.2.2 Rating of Resilient Features

The rating of resilient features for the Next Generation Nuclear Plant Project consists of two parts, as shown in EQN2. The first part provides a score (1-100) based on the reduction in risk score. The second part evaluates the synergistic collections of resilient features to verify that the selected collection of resilient features addresses each of the functions: anticipate, adapt, perceive, and respond.

$$RR = Ri \times (Ri - Rf) \quad [EQN\ 2]$$

Where:

RR = Risk Reduction Score

Ri = Risk Score prior to resilient feature = Ri

Rf = Risk Score resulting from added resilient feature.

Once the top resilient features are selected, each are grouped into collections of resilient features and rated for the synergistic ability, as follows in Figure 16:

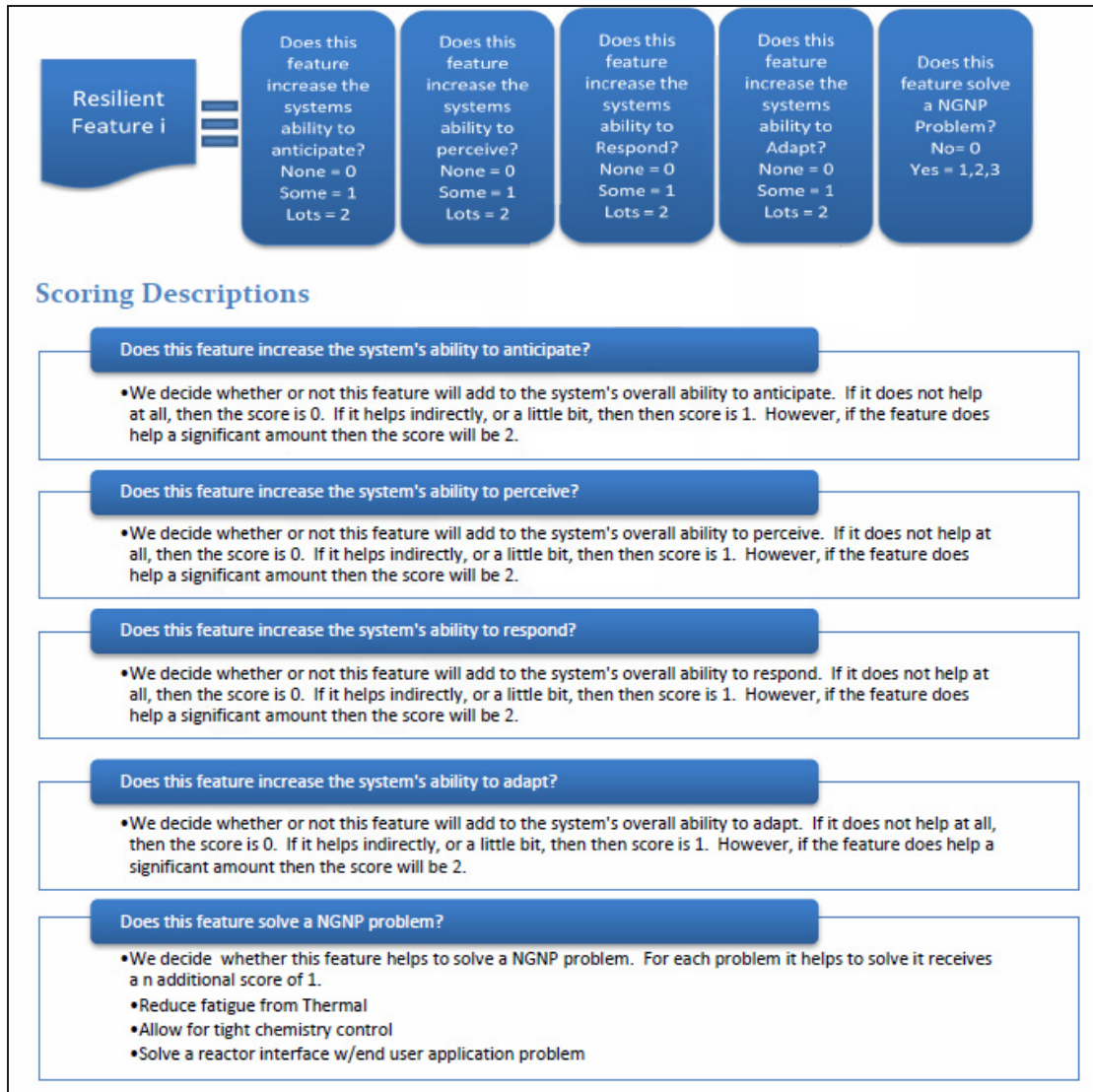


Figure 16. Resilient Features Scoring.

The Cobb-Douglass function (see EQN 3) allows one to evaluate the synergic extent of the four abilities and discount those collections of resilient features that do not provide at least some capability in each of the resilient abilities.

$$CR = A^{\alpha} \times AD^{\beta} \times P^{\gamma} \times RD^{\phi} \quad [\text{EQN 3}]$$

Where:

CR = Collective Resilience

A = Anticipate

AD = Adapt

P = Perceive

RD = Respond

$\alpha\beta\gamma\phi$  = weights of relative importance of the ability. Weights add to 1.

Thus, bundles of features that mitigate our chosen collection of consequences the most will have the highest consequence rating.

## **7.3 On-Going Research**

This section discusses current, on-going research being conducted at the INL in the area of control system design.

### **7.3.1 Resilient Control System Network Agents**

A large amount of effort has gone into detecting network attacks, including those specific to digital control systems. However, these solutions can become inefficient to monitor and maintain as they are dependent on signatures in the traffic that can provide copious false positives. Integrated cyber solutions are necessary to ensure that next generation reactors such as HTGR are not dependent on current bolt on cyber protections, such as the current nuclear fleet will be. This effort leverages the results of current research and commercial implementations to develop a software solution to detect and respond to unexpected control system security issues. The focus will be on change identification based on security incidents using intelligent anomaly detection algorithms that are flexible enough to identify emergent behavior. The use of intelligent agents that monitor digital control system hardware and react autonomously to changes in the status of the control equipment or its configuration, in cooperation with a cyber security system, is unique. These agents will be able to recognize abnormal behavior in network activity, specifically network intrusion signatures, and take action to preserve the integrity of the control components.

### **7.3.2 Wireless Sensor Testing**

Wireless sensor networks are becoming an integral component of process control in modern industry, but will require robust evaluation for implementation in an HTGR. Cost effectiveness is an important aspect of ensuring the acceptance of HTGR technology. However, RF and/or cyber interference to wireless sensors can potentially lead to destabilization of the control system by introducing latency or modifying data, which can undermine the control system design and amplify traditional concerns where impact is limited to the target of the interference. Therefore, to address this knowledge gap, the research proposed here is to design and analyze full-scale control systems that can be stressed by multiple interference types to develop approaches and solutions to resolve the expected system degradation and instability.

### **7.3.3 Integrated Control System Data Fusion**

Modern critical infrastructure control and security systems have the capability to provide facility managers, operators, and security personnel with an abundance of monitoring data. The current nuclear fleet will be limited to a segregated solution, which is dependent upon a number of personnel and working groups to independently analyze diverse data streams. This data comes from multiple sources, including process controls and physical and cyber security that are deployed at different levels within the system to provide both situational awareness and defense in depth. However, due to the complexity and amount of the data, it is challenging for operators to quickly analyze the situation and respond appropriately as they are inundated with too much data and not enough information. Due to this increasing volume of situational data and the potentially time-critical nature of decisions, data fusion emerges as a critical technology for transforming large amounts of information into timely, actionable intelligence. A holistic data fusion process that encompasses and prioritizes information from the sources mentioned above would enhance manager/operator response and increase overall facility stability and efficiency.

#### **7.3.4 Anomaly Detection, Diagnosis, and Resilient Control in Complex Engineered Systems**

One of the most important challenges for control system engineers today is how to design and implement intelligent, resilient control systems that will be robust to accidental and intentional abnormal events and assist operators in making supervisory control decisions for such abnormal situations. Events such as happened at the Three Mile Island station will not be acceptable under any circumstances, and an essential part of the protection for nuclear facilities and the correct interaction by its operators comes in the design of the control system. While limited diagnostic and prognostic technology is available in the current nuclear fleet, it is a bolt on solution with limited scope. In a resilient design, diagnostic and prognostic technology is an integrated solution that detects failure and presents it a uniform way. Thus, there is considerable incentive to develop intelligent resilient control systems that can provide automated operator assistance for supervisory control in complex nuclear facilities such as HTGR. The main objective of this effort is to develop a model-based hybrid framework for anomaly detection, diagnosis, and resilient control in complex process systems. This hybrid framework will integrate several recognized diagnostic and prognostic approaches for state awareness and model-based supervisory control, which overcomes the shortcomings of the individual components and is a significant advancement over the state-of-the-art.

#### **7.3.5 3-D Spatial Representation in Support of Design Inspection & Verification**

HTGR will be subject to safeguards via the International Atomic Energy Agency (IAEA). As a part of these safeguards, the IAEA performs design information verification (DIV) inspections to verify that facilities of interest have not been altered in any safeguards relevant manner that would allow misuse or diversion of special nuclear material. The practice of DIV relies heavily on inspector knowledge and experience and is performed within a highly information intensive environment. There are two fundamental difficulties when inspecting nuclear facilities. The first is sifting through facility documentation in search of relevant information (i.e., safeguards information), and the second is spatially correlating relevant information to the facility physical design. This project creates a facility information system (FIS) to address data storage and spatial registration of facility information, coupled with extraction of the relevant information on demand. Inspectors will interact with the FIS through a 3-D digital replication of the facility.

#### **7.3.6 Resilient Condition Assessment Monitoring (ReCAM) System**

This research considers resilient monitoring systems consisting of varying sets of multiple sensors in the interest of providing reliable assessment under any circumstance about the health of monitored processes. Considering a tightly coupled situation such as HTGR that is connected to varied fossil fuel processing and/or other users of high temperature heat, advanced control will be necessary to ensure the efficiency and stability of the integrated processes. However, advanced multivariable control will depend on multiple sensors that can fail, requiring a mechanism for graceful degradation. The objective of this research is to develop and demonstrate a rigorous framework and supporting algorithms for the implementation of condition monitoring systems that are both resilient and adaptive. This effort will involve developing an innovative architecture and its constituents, the notions of information quality (IQ) and assessment quality (AQ), and the methodologies for the effective deployment of resilient monitoring systems that can accommodate natural and malicious degradation. The resulting outcome of this research will lead to the autonomous selection of sensors and to a monitoring system that gracefully degrades (as opposed to collapsing) under perturbations.

#### **7.3.7 Automated Differential Equation-Based Identification**

In developing advanced control and prognostic methodologies, a first principles model is often needed. The fidelity of the control will be dependent on this model, which can be difficult to develop and define for new process technologies. Considering the implementation of advanced control for the new

HTGR processes, a necessary first step will require the formation of models that can then be used to develop suitable control algorithms. The research objective of this project is to explore the development of a new class of non-linear system-identification (SysID) methods that allows for the creation of non-linear differential equation-based models via attractor space reconstruction techniques using sample data from actual systems. This effort expands on previous work, which will be the discovery of unknown dynamical equations from hybrid energy systems. As such, efforts will involve performing state assessments and system prognostics for highly coupled, interdependent processing units.

## 8. CONCLUSION

This report has been prepared for the Next Generation Nuclear Plant Project to provide overall strategy for applying resilient controls to high temperature gas reactors. The functional analysis of the current state of traditional control systems and that of resilient control systems, identification of the gaps existing between traditional and resilient control systems that are most applicable to HTGR investment protection and operational efficiency, and the method used to identify and prioritize resilient functions for which HTGRs could most benefit from focused research and development, engineering analysis, and licensing awareness are also included in this document. By furthering the state of the art in resilient control systems and implementing selected resilient functions in HTGR design, it is anticipated that HTGRs will employ control systems that perform at higher levels, respond more quickly to disturbances, provide more efficient operations, and increase protection of HTGR investments.

The current fleet of LWRs employ a mix of analog and digital I&C. Safety significant systems use analog instrumentation and balance of plant systems have often been upgraded to digital I&C, some with advanced, separate from the system, bolt on measures such as cyber security. Upgrades to digital instrumentation and controls are guided by NRC's Regulatory Guide 1.152 but still lack the integrated benefits gained from a bottoms up design. With HTGRs in the early phases of design, strategic opportunities exist to provide an integrated, global approach to plant instruments, controls, and automation for increased efficiency and investment protection.

Unlike traditional control systems, resilient control systems of the future will be designed, installed, operated, and maintained to survive a natural disaster, human error, or intentional cyber attack with no loss of critical function. This is no small challenge in a sector that is complex, highly networked, and sensitive to the mildest failure. To achieve resilience and address the threats in next generation control systems, research is required to integrate an understanding of cyber security, human interaction, and complex network design. The integration of these three aspects will be introduced in the concepts of data fusion, mixed initiative, and hierarchical control system design.

An analysis of specific HTGR applications of resilient controls indicates additional research opportunities to advance the state of practice in resilience and prepare resilient methods for use in HTGRs. Resilient research areas of particular interest to HTGR investment protection include:

- Cyber and physical security,
- Process stability and efficiency,
- Integration of diverse indicators, and
- Interlacing of human and automatic responses.

HTGR control systems and their associated instrumentation must meet reliability, availability, maintainability, and resiliency criteria to achieve high capacity factors and remain economically competitive. Resilient control systems are one way of achieving the required availability by providing state awareness of all plant systems and their interactions and operational normalcy to allow for high capacity factors. The specific scenarios provided in this report demonstrate where resilient controls will



influence HTGRs by showing that control systems with adequate levels of resilience perform at higher levels, respond more quickly to disturbances, provide more efficient operations, and increase investment and public protection. A resilient strategy seeks to improve availability and enhance the economic competitiveness of the plant.

## 9. REFERENCES

1. *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434, U.S. Government Accountability Office, May 2005.
2. Craig G. Rieger (Idaho National Laboratory), "Control System," *Wikipedia*, <[http://en.wikipedia.org/wiki/Control\\_system](http://en.wikipedia.org/wiki/Control_system)>, Page last modified on 15 July 2010.
3. "Control System," *BusinessDictionary.com*, <<http://www.businessdictionary.com/definition/control-system.html>>, Page accessed on 25 August 2010.
4. Lynne M. Stevens, *Next Generation Nuclear Plant Resilient Control System Functional Analysis*, INL/EXT-10-19359, Idaho National Laboratory, Idaho Falls, Idaho, July 2010.
5. Craig G. Rieger (Senior Member, IEEE), *Notional Examples and Benchmark Aspects of a Resilient Control System*, 3<sup>rd</sup> International Symposium on Resilient Control Systems, Idaho National Laboratory, Idaho Falls, Idaho, August 10-12, 2010
6. Craig G. Rieger (Senior Member, IEEE), David I. Gertman, Miles. A. McQueen (Member, IEEE), *Resilient Control Systems: Next Generation Design Research*, HSI 2009: Conference on Human System Interaction, Catania, Italy, May 21-23, 2009.
7. INL, *Risk Management Plan for the Next Generation Nuclear Plant Project*, PLN-3247, Idaho National Laboratory, September 2009.
8. Erik Hollnagel, David D. Woods, Nancy Leveson (Eds), *Resilience Engineering: Concepts and Precepts*, Hampshire, England: Ashgate Publishing Limited, 2006.
9. NRC, *Regulatory Guide 1.152, Criteria for use of Computers in Safety Systems of Nuclear Power Plants*, Revision 2, U.S. Nuclear Regulatory Commission, January 2006.