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

ORNL/TM-2012/170

Advanced Control and Protection System Design Methods for Modular HTGRs

May 2012

Prepared by
T. L. Wilson, Jr.
S. J. Ball
R. T. Wood
M. S. Cetiner
W. P. Poore

UT-BATTELLE
ORNL-27 (4-00)

ORNL/TM-2012/170

Reactor and Nuclear Systems Division

ADVANCED CONTROL AND PROTECTION SYSTEM DESIGN METHODS FOR MODULAR HTGRs

T. L. Wilson, Jr., S. J. Ball, R. T. Wood, M. S. Cetiner, and W. P. Poore

May 2012

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

AOO	anticipated operational occurrence
AVR	Arbeitsgemeinschaft VersuchsReaktor
BDBA	beyond design basis accident
CCF	common-cause failure
DBA	design basis accident
DBE	design basis event
DOE	(U.S.) Department of Energy
EPA	Environmental Protection Agency
ESF	engineered safety function
FOAK	first-of-a-kind
HTGR	high-temperature gas-cooled reactor
HTTR	high temperature engineering test reactor (Japan)
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IHX	intermediate heat exchanger
INL	Idaho National Laboratory
LWR	light-water reactor
MCIG	miscellaneous control and instrumentation group
MCR	main control room
MHTGR	modular high-temperature gas-cooled reactor (DOE 1980s design)
NGNP	next generation nuclear plant
NPR	New Production Reactor
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
ORNL	Oak Ridge National Laboratory
PAG	Protective Action Guide
PCDIS	plant control, data, and instrumentation system
PD	proportional plus derivative (control)
PI	proportional plus integral (control)
PID	proportional plus integral plus derivative (control)
PPIS	plant protection and instrumentation system
PRA	probabilistic risk assessment
PSCS	plant supervisory control subsystem
PSER	preliminary safety evaluation report
PSID	preliminary safety information document
R&D	research and development
RCCS	reactor cavity cooling system
RSA	remote shutdown area
RTNSS	regulatory treatment of nonsafety systems

SCS	shutdown cooling system
SRDC	safety-related design condition
TRISO	trilayer isotropic (particle fuel)
VHTR	very high-temperature gas-cooled reactor

1. PROJECT OBJECTIVE

The project supported the Nuclear Regulatory Commission (NRC) in identifying and evaluating the regulatory implications concerning the control and protection systems proposed for use in the Department of Energy's (DOE) Next-Generation Nuclear Plant (NGNP). The NGNP, using modular high-temperature gas-cooled reactor (HTGR) technology, is to provide commercial industries with electricity and high-temperature process heat for industrial processes such as hydrogen production. Process heat temperatures range from 700 to 950°C, and for the upper range of these operation temperatures, the modular HTGR is sometimes referred to as the Very High Temperature Reactor or VHTR. Initial NGNP designs are for operation in the lower temperature range.

The following is a description of modular HTGRs taken largely from work by an International Atomic Energy Agency (IAEA) consultancy resulting in IAEA-TECDOC-1366[1] (August 2003). Characteristics are summarized as follows:

- high-quality ceramic-coated particle fuel of well-proven design, which adequately retains its ability to contain radioactive fission products over a wide range of conditions;
- single-phase helium coolant, with no heat transfer limits associated with phase change and no phase change over the full range of possible normal or off-normal conditions;
- passive post-shutdown decay heat removal achievable through conduction, natural convection, and radiation heat transfer, limiting maximum temperatures to values consistent with coated-particle fuel performance limits for retention of radionuclides;
- combination of low-core power density, high reactor core and internals heat capacity, high-core thermal conductivity, and large fuel thermal margins, resulting in very long times (days) for evolution of responses to loss-of-normal operation functions without protective actions; and
- fuel temperature margins and negative temperature-reactivity coefficients sufficient to accommodate foreseeable reactivity insertions during startup and power operation without damage to the fuel.

The defining safety characteristic of the modular HTGR is that its primary defense against serious accidents is to be achieved through its inherent properties of the fuel and core. Because of its strong negative temperature coefficient of reactivity and the capability of the fuel to withstand high temperatures, fast-acting active safety systems or prompt operator actions should not be required to prevent significant fuel failure and fission product release. The plant is designed such that its inherent features should provide adequate protection despite operational errors or equipment failure.

Figure 1 shows an example modular HTGR layout (prismatic core version), where its inlet coolant enters the reactor vessel at the bottom, traversing up the sides to the top plenum, down-flow through an annular core, and exiting from the lower plenum (hot duct).

This research provided NRC staff with (a) insights and knowledge about the control and protection systems for the NGNP and VHTR, (b) information on the technologies/approaches under consideration for use in the reactor and process heat applications, (c) guidelines for the design of highly integrated control rooms, (d) consideration for modeling of control and protection system designs for VHTR, and (e) input for developing the bases for possible new regulatory guidance to assist in the review of an NGNP license application. This NRC project also evaluated reactor and process heat application plant simulation models employed in the protection and control system designs for various plant operational modes and accidents, including providing information about the models themselves, and the appropriateness of the application of the models for control and protection system studies.

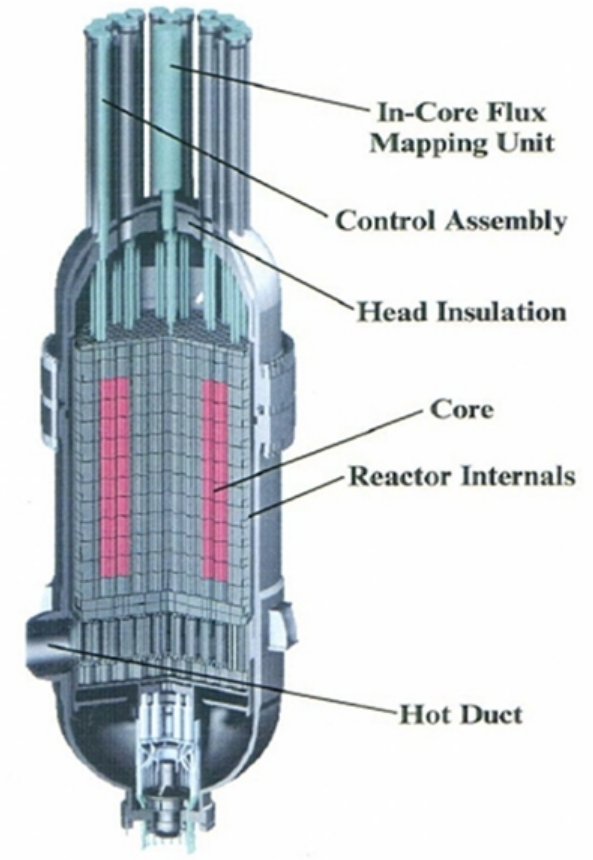

Fig. 1. Modular HTGR reactor vessel (prismatic core).

A companion project for the NRC focused on the potential for new instrumentation that would be unique to modular HTGRs, as compared to light-water reactors (LWRs), due to both the higher temperature ranges and the inherent safety features.[2]

The four informal reports that this overview report summarizes are:

1. *Task 1—Control and Protection Systems in VHTRS for Process Heat Applications,* LTR/NRC/RES/2010-001,
2. *Task 2—Highly Automated Control Room Design for VHTRS,* LTR/NRC/RES/2011-005,
3. *Task 3—Models for Control and Protection System Designs in VHTRS,* LTR/NRC/RES/2011-003, and
4. *Task 4—Advanced Control and Protection System Design Methods,* LTR/NRC/RES/2011-008.

1.1 MODULAR HTGR CONTROL

1.1.1 Heat Transport System Control during Normal Operation

The unique features of modular HTGR plant control mainly involve the control of its heat transfer processes. The high-temperature, high-pressure helium coolant removes the core heat by convection and transports it to a heat exchanger, steam generator, or gas turbine. Secondary or tertiary loops, if they are part of the design, further convey the heat to other devices such as turbines or other energy conversion–related processes. At steady state, the operational control system regulates the processes to the specified setpoints of the design. The automated controls adjust for load perturbations as well as gradual changes in the plant such as fuel burnup, steam generator fouling, or changes in the temperature of the final heat sink. Feedback control is used to regulate temperatures, flows, and pressures within the heat transport system to their setpoints, compensating for all of these variations.

The control system is also responsible for normal maneuvering, including startup and shutdown, major changes in load from one power level to another, and for restoring the plant to an equilibrium state following major disturbances such as a turbine trip or feedwater pump trip.

Many aspects of modular HTGR heat transport system controls are quite different from those of LWRs. First, the mean temperature rise of the coolant through the core is ~400°C, or about a factor of 10 larger than for LWRs, so system temperature gradients are much larger. Since the mean coolant outlet temperature is very high, it is important that it remains constant (high) over the power operating range both to maintain high efficiency and avoid thermal cycling of the high-temperature components. The inlet coolant temperature should remain nearly constant as well in the 300–400°C range. This is because the inlet coolant is used to maintain moderately low reactor pressure vessel temperatures by cooling the vessel in its path from the reactor vessel entrance up to the top (inlet) plenum. Thus, for variations in power (load) from 100 to 20%, the mass flow rate of the coolant must also change from 100 to about 20%. This would increase thermal response time constants by about a factor of 5 as well. Another feature of the core coolant is the large spatial variations in outlet temperatures due to uneven heating, on the order of ~100°C or more. The resulting mixing problems (including temperature sensor signal fluctuations) can make it very difficult to get valid mean temperature measurements for this important control signal.

The control strategy for normal operation and regulation of the heat transport systems involves controller designs that are similar to those for conventional power plants. The algorithms typically use single loop controls with proportional–integral or proportional–integral–differential action. In many instances, feedforward inputs are added to the feedback action to improve coordination between the different parts of the heat transport system and to improve the speed of response, keeping the different parts of the heat transport system responding in a prompt but stable manner. For feedforward action, the control system employs a two-level cascade in which a top level controller computes a setpoint for the lower level controller. The lower level controller in the cascade forms a second error using another measured variable in its feedback loop. The output from the lower level controller is an actuation signal (increase/decrease) or a position demand.

In a typical two-level cascade control loop with feedforward action for demand output (or an increase/decrease output—see Fig. 2), the demand output is used by actuators such as valve positioners or by systems such as rod controllers. The feedback devices are shown as having proportional–integral action but could be any combination of proportional, integral, or differential action.

The first-level feedback gives the corrective action for deviations due to variations in the process. If integral action is included in the first controller, then the cascade setpoint integrates to a value that yields zero offset in the first-level error. Typically, this integral has a low gain for a slow, stable approach to steady state and is tuned on the basis of the time constant of the first-level measured variable to the system demand.

The second-level feedback error takes advantage of a measured variable that is more directly affected by the actuator to provide rapid positioning. The open loop response from the demand to the second-level measured variable is usually quite fast. The control gains can be much larger, which improves the tracking of the final demand to the feedforward signal.

As an example, assume the first-level measured variable for rod control is the average core outlet helium temperature signal, which has a slow response to power level changes. The low-gain integral action applied to the temperature error signal responds to load changes and corrects for gradual effects such as fuel burnup, errors in feedforward signal, and other disturbances so that the reactor outlet temperature stays at the operating point. The second level, or inner loop measured variable, is neutron flux, which responds much more rapidly to control rod motion. Rod control at the lower level causes the neutron flux to track the load demand in unison with circulator speed, feedwater flow, and turbine response.

Although the cascade structure results in what is actually a multivariate control problem, analytical methods of modern control have not typically been applied to determine the gains. Instead, trial-and-error methods of manual tuning or approximate methods such as Zeigler-Nichols are typically employed to adjust the gains of the cascade. Likely this is because conventional tuning strategies have worked well. The complexity of the modern multivariate control system design has not yet been justified. Based on a survey of the literature, control schemes for HTGRs appear to be developed with ad hoc structure and trial-and-error tuning.

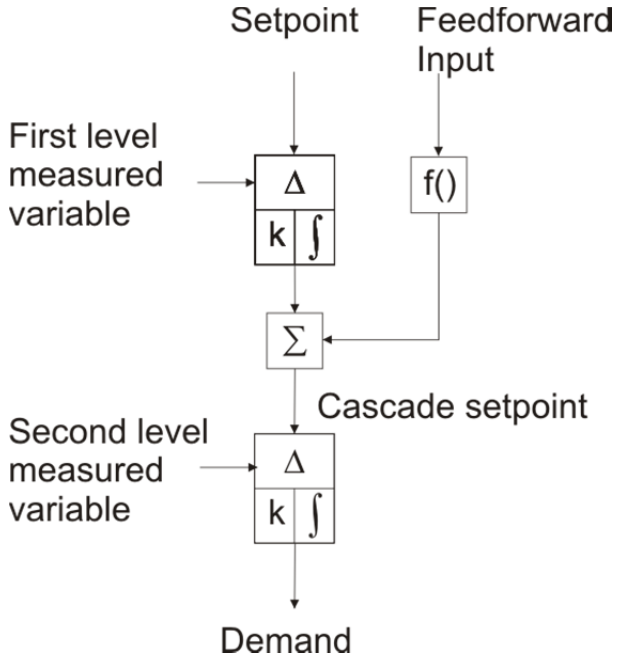

Fig. 2. Two-level cascade controller with demand output.

1.1.2 Steam Generator–Turbine Heat Transport Controls

Four different HTGR designs were studied to compare heat transfer control schemes and the benefits and limitations of each. These were

- Fort St. Vrain Nuclear Generating Station (Public Service Company of Colorado),
- MHTGR (Modular HTGR—U.S. DOE design, circa 1980),
- AVR (Arbeitsgemeinshaft Versuchsreaktor, Germany, 1963–1988), and
- HTTR (High Temperature Engineering Test Reactor, Japan).

Comprehensive descriptions of these reactors are given in the IAEA TECDOC-1198[3] and the *Nuclear Engineering and Design* article on the AVR.[4] Three of the four HTGR designs surveyed have a steam generator and steam turbine for power conversion. The fourth (HTTR) has a water-cooled heat exchanger that dumps heat to an air cooler. The heat transport elements of the steam generator plants consist of the reactor, helium circulation system, the steam generator, and the steam turbine–generator. The heat transport system inputs and outputs are all closely coupled together, and many different input–output pairs give feasible control systems.

Three of the steam generator–turbine plants surveyed have sufficient detail to compare overall control schemes for the heat transport control. The main heat transport loop at normal power operation involves control variables for four main systems—reactor power, feedwater control, electrical power, and circulator flow. The control schemes are compared in Table 1. What is interesting is that substantially the same control problems can be solved in three very different ways for these three reactors.

The table gives the specific input and output variables for each loop in terms of the cascade controllers. For example, the column for the MHTGR indicates that the first-level process variables are assigned so the allocated load (for each reactor module) is controlled by the module feedwater flow valve, the steam pressure (for a power block) is controlled by the turbine throttle valve, and steam temperature is controlled jointly by circulator speed and reactor neutron power. The MHTGR uses the measured feedwater flow setpoint as a feedforward input to coordinate the reactor power and the circulator speed. The input/output pairs and actions are based on the operational descriptions of the control systems. Some uncertainty in the data exists because of vague descriptions in the source documents. Questionable data are indicated with (?).

Table 1. Cascade control schemes for three HTGRs*

Controlled variable	Controller input components	MHTGR	Fort St. Vrain	AVR
Control rods	Feedforward input	FW flow	Steam flow	None
	First level (action)	Steam temperature (PD or PID)	Reheat steam temperature (PI)	Reactor outlet temperature (Manual?)
	Second level (action)	Neutron flux (P)	Neutron flux (P)	None
	Output	Increase/decrease	Increase/decrease	Increase/decrease
Helium circulator motor frequency	Feedforward input	FW Flow	FW flow	None
	First level (action)	Steam temperature (PD)	Main steam temperature (PI)	Electrical load (Manual?)
	Second level (action)	None	None	None
	Output	Speed demand	Speed demand	Speed demand
Feedwater valves	Feedforward input	Module load	Turbine first stage pressure	
	First level error (action)	FW flow (PI)	Steam pressure (PI?)	Steam temperature (Manual?)
	Second level error (action)	None	FW flow (PI?)	None
	Output	Valve demand	Valve demand	Valve demand

Table 1. Cascade control schemes for three HTGRs* (continued)

Turbine admission valve	Feedforward input	Total load	None	None
	First level error (action)	Steam pressure (P)	Electrical load	Steam pressure (P)
	Second level error (action)	None	None	None
	Output	Increase/decrease	Increase/decrease	Increase/decrease

*PD = proportional plus derivative (control); PID = proportional plus integral plus derivative (control); PI = proportional plus integral (control); P =proportional (control)

Figure 3 shows the control system diagram for the MHTGR. Note that the reactor temperature control system uses the measured steam temperature (outlet from the steam generator) instead of a signal from the primary system helium outlet from the reactor vessel, most likely due to the potential reliability and accuracy problems with the helium outlet temperature sensor.

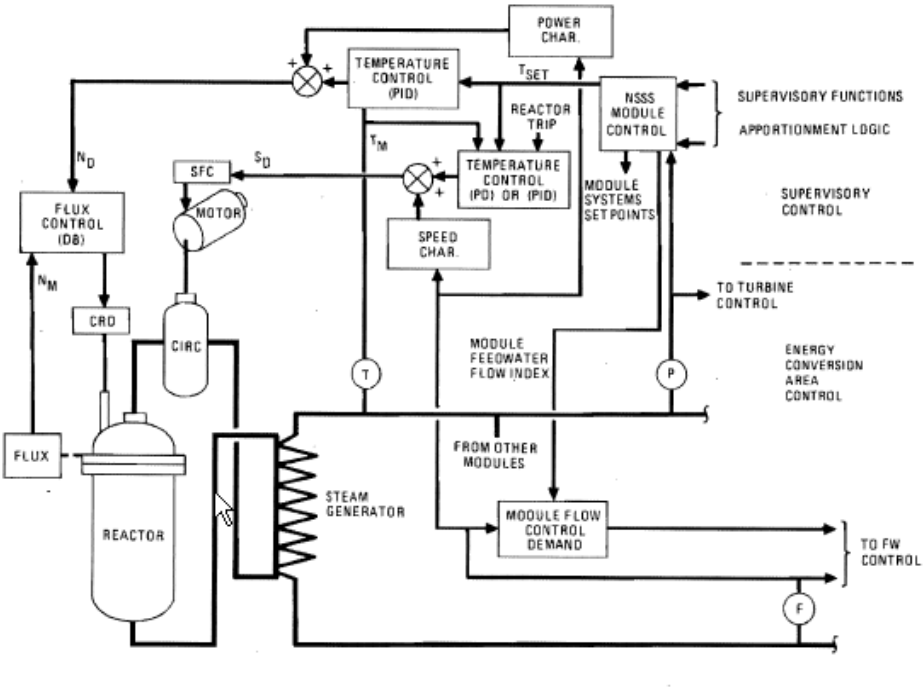

Fig. 3. Control subsystem functions and interfaces for the MHTGR.[5]

1.1.3 Direct-Cycle Gas Turbine Plants

The other major type of power conversion proposed for modular HTGRs is the direct-cycle gas turbine. These designs have higher projected efficiencies than steam generator designs and avoid many operational complications, much of the radioactivity exposure (to operators), and potential steam ingress accident concerns common to the direct-cycle steam generator plants. The most common configuration for the plants is a single shaft design in which the compressor, turbine, and generator are all on the same shaft. This arrangement allows using the generator as a motor for startup. The control inputs are considerably different from those in a steam turbine plant. In normal operation, when the generator is synchronized to the grid, the helium circulator speed is fixed by the grid frequency. Also, the gas turbine is not usually throttled like steam turbines. Lacking the independent circulator speed and turbine throttle valve action takes away two degrees of freedom that the steam generator plants utilize. The control inputs

for the gas turbine system are the rod position, helium inventory (mass in primary), turbine bypass valve, and the intercooler flow control valve.

The turbine bypass valve routes the helium flow around the turbine. It is a fast-acting, but thermodynamically inefficient, means for controlling electrical load. Helium inventory control is the slow-acting means for controlling electrical load. Changing the density (average pressure) of the helium coolant allows for maintaining the same gas velocities and blade vs gas velocity angles so that the high efficiency is maintained with load (electrical power output) changes. The helium flow to the inventory storage system is extracted from the high-pressure side of the compressor, and return flow is to the low-pressure side; hence, no separate helium pump is needed (except for startup). The control rods are used to control reactor outlet temperature (with the cascade control noted earlier), and the intercooler secondary side cooling water flow rate is used to control reactor coolant inlet temperature.

1.1.4 Helium Purification Systems

Helium purification systems contain a number of local controls for controlling the flow and temperature of the helium stream. In addition, the normal operation of these systems typically has two submodes—purification and regeneration. Helium purification systems have at least two trains so that one train can be online and processing the helium coolant and the other in regeneration to remove impurities from adsorption beds and ready them for reuse. Automatic controls for both normal purification and regeneration would involve on/off controls to redirect flows and transfer systems from one mode to the other and control algorithms to regulate temperatures, flows, and chemical concentration in the purification and regeneration modes. Control scheme details for the purification systems were not found in the literature survey.

Moisture removal from the primary system is one of the safety functions required following water ingress events or other leakages.

1.1.5 RCCS Control Systems

The reactor cavity cooling system (RCCS) for modular HTGRs is typically a safety-grade system, either with passive or highly reliable, redundant forced-convection cooling systems designed to remove core afterheat in case of failure or unavailability of the main and all other active shutdown cooling systems during accidents. It also serves as the cooler for the reactor cavity concrete and other critical equipment in the cavity. The requirements for RCCS performance and reliability may vary considerably depending on the particular reactor design features, power level, materials, containment type, and investment protection or licensing considerations. In some cases, these requirements could be extremely stringent if afterheat removal is the critical factor in determining maximum design power level and the need (or not) for a sealed containment structure. A common solution to the problem of ensuring adequate heat removal is to overdesign (the capacity of) the system. This would not normally be acceptable for the RCCS, however, because during normal operation, excessive parasitic heat losses are undesirable.

For “completely passive” RCCS designs, there would be no control system involved, but its performance during normal operation would be monitored to ensure availability in case of an accident (as well as its functioning to protect reactor cavity components and concrete from overheating). In designs for which the RCCS employs forced cooling during normal operation but “switches” to passive operation upon loss of power, some control features would be necessary. The objective would be for the control to “fail safe.”

1.1.6 Conventional Cooling Systems

Controls for support cooling systems such as a vessel cooling system, shutdown cooling system, component cooling system, and various balance of plant heater exchangers require normal controls similar to LWRs. Detailed descriptions of the controls and instrumentation for these systems were not found in the literature survey.

1.1.7 Potential NGNP Heat Transport Systems Controls

In an early NGNP project design, the concept was that a hydrogen production plant would be the only heat load. A combined-cycle plant involving, for example, both electrical generation and hydrogen production was not planned. However, the NGNP design is still in a state of flux. A number of key design issues for the control system, including the heat load configurations, are undecided. The control issues will, of course, depend significantly on the resulting plant loop configurations.

Designs involving intermediate loops for driving steam cycle, combined electrical load and chemical plant, and direct-cycle gas turbines have been proposed. The range of possibilities does not lend itself to a useful general discussion of controls and protection. Each type of heat load [i.e., steam generator and turbine, gas turbine, or a process heat plant coupled via an intermediate heat exchanger (IHX)] typically has a set of measured variables and control requirements, making its behavior independent of the other heat loads in a combined-cycle plant. The combined-cycle plant requires additional control logic to allocate the reactor heat source to the individual heat loads. The transient analysis of combined-cycle plants must include all the potential transients each heat load can initiate and their impacts on the heat source and the rest of the plant. The complexity and diversity of potential load variations impact both the controls and protection systems designs.

2. NGNP PROTECTION STRATEGY

The protection strategy of a nuclear power plant consists of the set of designed responses that protect the plant from postulated disturbances and equipment failures or malfunctions, ultimately preventing releases of radioactive materials from the fuel. The disturbances and failures upon which the strategy is based are typically classified in three major event frequency based categories—anticipated operational occurrences (AOOs), design basis accidents (DBAs), and beyond design basis accidents (BDBAs). AOOs are defined as conditions or upsets of normal operation that are expected to occur one or more times during the life of the plant. DBAs, which are not expected to occur during the lifetime of the plant, are conditions against which the plant is designed to keep release of radioactive material within regulatory limits. BDBAs are very unlikely events, more severe than the DBAs, where the very rare events are allowed higher release consequences.

The protection strategy is created as a response to the events as a way to protect against adverse consequences and, thus, has a central role in the protection design process. Once the safety strategy is conceived and demonstrated by safety analysis to protect the plant and public, the strategy must be implemented in the software and hardware of the safety system's I&C design. The licensing test for the I&C system is to show that the actual system performs as well as or better than the protection strategy used in the safety analysis with its conservative assumptions. In this report, the assumed design is the baseline NGNP with a single reactor driving a steam generator and turbine generator.

A comprehensive description of the events that are likely to be considered for the NGNP is given in the IAEA Safety Report Series No. 54, *Accident Analysis for Nuclear Power Plants with Modular HTGRs.*[6] The list and descriptions provide a basis for discussing necessary protection functions for the NGNP and notes contrasts with LWR protection strategies.

2.1 INSTRUMENTATION AND CONTROLS FOR PROTECTION SYSTEM FUNCTIONS

NGNP safety systems are likely to be similar in structure and hierarchy to existing digital safety systems because simplicity and reliability require it. Innovation and complexity are not normally advantages. It is to be expected that the logic in the safety system consists of an envelope of operating conditions within

which the plant is ensured by safety analysis to be protected. Unsafe conditions and equipment failures will be detected by measured parameters reaching a trip setpoint at the edge of the safety envelope. The trip logic will seal in, and a function or set of functions will be initiated to drive the plant to a safe shutdown state. The safety analysis is used to show that all credible events are detected by the envelope and comparator logic and that safety functions can safely mitigate the event.

While the envelope concept of a protection system is expected to be the same as that for a traditional plant, there may be some new features not present in existing plants. Resilient control and trip avoidance measures[7–10] are features intended to improve safety and increase plant availability. The resilient controls would act inside the traditional safety envelope. For example, the control system may employ trip avoidance strategies to reduce the demands on the protection system. Using resilient control techniques, the controls system may automatically diagnose equipment degradation or failures and reconfigure the operating controls to adapt to the degraded conditions. The "resilience" is to maintain the reactor in safe operating condition without having to exercise the protection system, to increase reliability and availability of the plant, and to minimize thermal transients that could stress the reactor systems. The difficulty is the complexity of the resilient control scheme and the potential for adverse, unforeseen interactions between the resilient control and the protection system. The difficulty is not all that unforeseen. In fact, the strategies are geared to make adverse interaction unlikely. However, it is difficult to prove that a complex system has no adverse interactions with the level of certainty needed for reactor safety. This report leaves as an open issue the problems of licensing resilient control and trip avoidance. Since the proposed use of resilient control has not moved yet to even a conceptual design phase, the question cannot be very well evaluated.

The following section provides a discussion of the logic functions that seem likely candidates for the protection of the baseline NGNP. The logic for each safety function is hypothetical; however, the purpose of presenting hypothetical logic is for discussion of potential problems and licensing differences with respect to LWRs since the actual NGNP protection logic has not yet been designed.

2.1.1 Reactor Scram Logic

The following plant states are used by the plant protection system to initiate the automatic reactor scram logic:

- manual,
- low main steam line pressure,
- low hot reheat steam pressure,
- high wide-range channel rate of neutron flux change,
- high startup count rate (startup only),
- rate of change of startup count rate (startup only),
- neutron flux high,
- high moisture in the primary coolant,
- high reheat steam temperature,
- low primary coolant pressure (only at power),
- high primary coolant pressure,
- plant electrical system power loss,
- high reactor building temperature,
- high reactor building pressure,
- circulator trip, and

- auxiliary scram actions (e.g., turbine trip).

2.1.2 Reactor Cavity Cooling System (RCCS)

The RCCS is the only safety-related heat removal system. (The steam generator and the shutdown cooling system are typically nonsafety heat removal systems.) The totally passive RCCS (in most designs) is always on and does not have any logic for initiating the function. The RCCS only requires monitoring of temperatures to ensure normal operations are proceeding. Those RCCS designs having active cooling systems during normal operation would need to have safety-grade systems to ensure a proper transfer to the passive mode under postulated accident conditions.

2.1.3 Circulator Trip Logic

The NGNP circulator is expected to be a variable-speed electrically driven blower. Trip functions are to protect against overcooling and against circulating air or moisture in the event of an ingress event. The circulator trip provides a backup shutdown mechanism since the decreased heat removal allows temperature to rise effectively shutting down the nuclear reaction through the strong negative temperature coefficient.

The plant protection system may use these parameters in circulator trip circuit and provide an input to the reactor protection system:

- manual,
- low circulator speed,
- high circulator speed,
- low feedwater flow,
- low circulator magnetic bearing clearance,
- reactor trip,
- turbine trip,
- circulator penetration pressure high,
- steam leak detection (turbine building pressure, rate of rise),
- steam leak detection (reactor building pressure, rate of rise),
- steam leak detection (turbine building pressure, fixed setpoint), and
- steam leak detection (reactor building pressure, fixed setpoint).

2.1.4 Circulator Start Inhibit Logic

The circulator may be inhibited from starting if core temperatures are too high and there is a potential problem with damage to structural materials downstream of the core.

2.1.5 Rod Withdrawal Prohibition Logic

The rod withdrawal prohibition logic prevents large reactivity insertions in approaches to critical during startup or an overpower event during power operation.

The NGNP plant protection system may use these parameters in rod withdrawal prohibition:

- low count rate,
- high startup range channel rate of neutron flux change,
- high wide range channel rate of neutron flux change,

- high flux level,
- flux-to-flow ratio interlocks,
- rod control circuit load, and
- power range failure.

2.1.6 Reserve Shutdown System and Safety Shutdown Cooling System Logic

The NGNP reserve shutdown system and safe shutdown cooling systems are expected to be manually actuated with no operating bypasses. Instrumentation for operator control information is required. The shutdown system requires monitors of position of the release mechanism and detection that absorber balls have been released. The shutdown cooling system needs monitoring of the shutdown circulator, helium coolant temperatures, temperatures and flows in the shutdown heat removal heat exchanger, and coolant pressures. Isolation of the shutdown cooler is an ESF (engineered safety function).

2.1.7 Steam/Water Dump

The steam dump system isolates and drains the steam generator with a tube leak to limit the amount of water in the steam generator that could enter the primary. Upon detection of excess moisture in the primary, the dump system activates emergency feedwater isolation valves and main steam stop/check valves. The dump is accomplished by the rapid opening of two parallel redundant valves relieving water and steam through the feedwater header to the dump tank. To meet redundancy requirements, either valve must be sufficient to drain the steam generator.

2.1.8 Steam Generator Isolation

Actuation of steam and feedwater block valves are ESF functions required for preventing water and steam entry into the steam generator when a tube leak is detected. The isolation is initiated in response to moisture in the primary.

2.1.9 Confinement Vessel Pressure and Filtration Flow Logic

The confinement building in most proposed NGNP designs is a low-pressure-sealed building (Vented Low Pressure Confinement), which would be a departure from the thick-wall, high pressure containment of LWRs. The safety benefits of the VLPC compared to those of a high-pressure containment are not immediately obvious. The premise for the VLPC is that an early gas release from a break in the primary pressure boundary would be low in contamination. An early relief of this gas from the VLPC removes the potential for a high energy driving force (from the pressurized gas in a high pressure containment building) if the accident continued for a long time until fuel failures did occur. To protect the VLPC from overpressure, the building must release helium to atmosphere. In the proposed concept high pressure is relieved by passive damper panels that act as low pressure check valves.

Active controls are needed for controlling temperature and flow to filtration system that would be used for accident mitigation and recovery. The filtration function is triggered by the following indications that contaminated primary coolant is entering the confinement:

- high reactor cavity activity and
- high cavity pressure.

2.1.10 Plant Protection, Instrumentation, and Control Systems for the MHTGR

The 1980s DOE design of the MHTGR provided for interconnected and integrated automatic control of four reactor modules and two turbogenerator systems comprising the plant. Automatic control is used for normal operations and for abnormal events; no operator actions are required to shut down the reactor for event categories included in the safety analysis. The plant safety/protection function is provided by separate, redundant safety-related instrumentation and control components. The plant is to be controlled by an operator and an assistant from the main control room. Additional monitoring and control capabilities are provided at a remote shutdown area room in the reactor service building and in plant protection and instrumentation system rooms in each reactor building. A description of the protection and I&C systems for the MHTGR is summarized in the NRC's draft preliminary safety evaluation report (PSER) as well as concerns resulting from the staff review of the preliminary safety information document (PSID). An overview of this NRC assessment is provided in this section.

MHTGR plant protection and automatic control are provided by the partly safety-related plant protection and instrumentation system (PPIS); the plant control, data, and instrumentation system (PCDIS); and the miscellaneous control and instrumentation group (MCIG).

The MHTGR instrumentation and control system has several novel features compared with the existing reactor fleet.

- All four reactor modules and the two turbine generators are monitored and controlled from a single control room via a modular, distributed control system that allows load to be allocated automatically among the reactor modules and the two turbine generators.
- An independent, redundant, and fully automated protection system, including a remote shutdown area, is provided. The safety-related portions of the system (reactor trip and main coolant loop shutdown) are fully automatic; no safety-related operation actions are necessary or are even available in the control room.
- Most of the PPIS circuitry is contained in reactor module equipment rooms. The control room is not deemed as safety related by the applicant.
- Control room operator actions are not viewed as safety related but as a monitoring function and performance of plant mission management activities.
- Manual initiations of protective functions may be carried out in the remote shutdown area (RSA) or reactor module PPIS equipment rooms.
- The control room, RSA room, and reactor module PPIS rooms are designed to limit operator exposures during accident conditions.

2.1.11 Plant Protection System

The PPIS indicates plant status and automatically actuates safety-related control systems and investment protection control systems. It consists of the safety protection, special nuclear area instrumentation, and investment protection subsystems.

2.1.11.1 Safety protection system

The safety protection subsystem initiates a reactor trip and shuts down the main cooling system. Specifically, the subsystem initiates

- a reactor trip with the outer control rods,
- a reactor trip utilizing the reserve shutdown control equipment—a diverse trip system, and
- a main loop shutdown and isolation of main steam to protect against water ingress events and to protect major secondary-side equipment.

Note that in more recent designs of modular HTGRs, the reserve shutdown system is activated only by operator action. The safety protection subsystem is classified as safety related. It has the capability to sense plant process variables, detect abnormal plant conditions, and initiate protective actions. The scope of the system begins with process protection sensors and extends to the inputs of actuated systems. The system mitigates the consequences of design basis events to protect the public health and safety and to ensure that equipment and structure damage limits are not exceeded. Redundancy is employed within the safety protection system of each module. Each module has a separate and independent, remote multiplexed, centrally controlled, microprocessor-based safety protection system. As originally planned, separate and independent safety protection system operator interfaces for each reactor module were to be provided in the plant's remote shutdown building. Ultimately, this capability would likely have been extended to the main control room at the request of the NRC. Its architecture consists of multiple separate and redundant optical-digital-data pathways from the remote multiplex units that communicate with four separate, redundant computers that make up the four-channel protection systems for each module. Two-out-of-four coincidence logic initiates a protective action.

The first protective action is the trip of a reactor module's outer control rods, which can occur for safety-related or nonsafety-related plant conditions. Safety-related conditions are

- neutron flux to helium mass flow ratio—high,
- primary coolant pressure—high, and
- primary coolant pressure—low (bypassed on low neutron flux).

Nonsafety-related conditions for which the safety protection system actuates are

- primary coolant moisture concentration—high,
- steam generator helium inlet temperature—high,
- main loop shutdown/main steam isolation trip signal, and
- manual actuation.

A reactor trip signal also notifies the plant data, control, and instrumentation system to initiate a feedwater flow reduction and ramp down of the steam supply system.

The second protective action is to actuate the reserve shutdown control equipment, which occurs if the outer control rod trip system fails when commanded or if there is a positive reactivity condition due to water ingress into the core that exceeds the negative reactivity of the outer control rods. Safety-related conditions are

- neutron flux to main circulator speed—high (with a time delay to allow for outer rods to trip),
- primary coolant pressure—high, and
- manual actuation (a nonsafety-related condition).

The reserve shutdown control equipment initiates when the actuation signal causes fusible links to be energized and opened, which causes hoppers of borated pellets above the core to empty their contents into empty channels in fuel columns adjacent to the inner reflector, adding negative reactivity to the core. The negative reactivity of the reserve shutdown system is sufficient alone to maintain the required level of subcriticality at cold shutdown and maximum water ingress.

The third protective action is the main loop shutdown and main steam isolation. This main steam isolation/steam generator isolation limits chemical attack on the fuel from water ingress to the core from a steam generator leak and protects the turbine from low-temperature, low-quality steam. The main loop shutdown protects steam generator components from excessive primary system temperatures. The loop shutdown occurs when the main circulator receives a trip signal and feedwater block valves are signaled to close. Concurrently the main steam isolation valves shut off the secondary coolant system loop. Conditions requiring main loop shutdown are

- primary coolant pressure—high (safety-related condition),
- circulator speed high or low compared to a programmed setpoint (a nonsafety-related condition),
- steam generator isolation and dump signal (a nonsafety-related condition), and
- manual actuation (a nonsafety-related condition).

Conditions requiring main steam isolation are

- main loop shutdown (safety-related condition),
- main steam low temperature (a nonsafety-related condition), and
- manual actuation (a nonsafety-related condition).

2.1.11.2 Special nuclear area instrumentation subsystem

The functions of the nonsafety-related (as proposed) special nuclear area instrumentation subsystem include

- primary system pressure relief block valve closure interlock,
- protection subsystem information displays, and
- post-accident monitoring instrumentation.

2.1.11.3 Investment protection subsystem

The investment protection subsystem monitors plant conditions and initiates protective actions to limit plant investment risk. It was proposed as a nonsafety system whose functions include

- reactor trip with inner control rods,
- steam generator isolation and dump,
- shutdown cooling system initiation,
- primary coolant pump-down, and
- shutdown cooling heat exchanger isolation.

Operator interfaces for investment protection systems are located in the safety protection equipment rooms, the main control room, and remote shutdown areas/rooms. An operator may initiate reactor trips and main cooling system shutdown using the investment protection subsystem from the remote shutdown areas, separate from the main control room. In the proposed design, manual inputs (e.g., manual reactor trips) to the safety protection system cannot be made from the main control room; however, a normal shutdown can be accomplished from the main control room. The operator interfaces for investment protection are separate and independent of all other plant instrumentation and controls.

The NRC staff voiced several concerns during their review of the pre-application safety information document to be examined in more detail when the full application is submitted. These included the means for an operator to manually trip the reactor, ensuring independence of the protection system from the control system, nonsafety classification of certain equipment (such as investment protection trip functions that are common to the safety-protection trip functions), the block valve closure interlock system, steam generator dump and isolation valves, and system monitoring equipment.

2.1.11.4 Plant control, data, and instrumentation system

The MHTGR's nonsafety-related plant control, data, and instrumentation system (PCDIS) is a network of integrated, hierarchical digital computers and control and monitoring instrumentation that permits the modular reactor units and two turbine generators to be operated and controlled from startup to power operation to normal shutdown. It is comprised of four subsystems: (1) plant supervisory control subsystem (Fig. 4), (2) nuclear steam supply control subsystem, (3) energy conversion area control

subsystem, and (4) data management subsystem. The descriptions provided below were extracted from *Plant Protection, Instrumentation, and Control.*[11] Changes in various design choices may have superseded some of the information presented here; however, the basic philosophy still illustrates the system principles.

2.1.11.5 Plant supervisory control subsystem

The plant supervisory control subsystem (PSCS) coordinates plant control during operation, shutdown, refueling, and startup/shutdown. The PSCS determines how to apportion overall plant load demand to individual reactor modules and turbine generators. It determines main steam and feedwater flow rates necessary to meet load maneuvers that may originate with the plant operator, grid operator, or reactor module or plant conditions. The PSCS computers manage the plant through selection of the necessary mode of plant operation and control strategy for best operation of the reactor modules and turbine generators independently at various power levels, and then validate the appropriate plant response. The PSCS has startup/shutdown, normal operation, refueling, shutdown, and abnormal operating modes. The control strategies associated with each operating mode are briefly described.

2.1.11.5.1 PSCS startup/shutdown

Table 2 summarizes the PSCS control strategy during plant startup and shutdown. Reactor module startup from depressurized shutdown consists of bringing the modules up to minimum stable operating conditions sequentially through a series of operator checkpoints several times during the startup. These checkpoints are underlined in the table.

Load levels for the modules are raised in parallel to a common average level at ramp rates of +0.5% per minute. Modules are connected to the main steam header one at a time. The logic for shutdowns is the reverse of startups. For shutdowns, the modules are shut down in a parallel manner at incremental levels. Modules are disconnected from the main steam header one at a time.

Table 2. PCSC control strategy for normal startup or shutdown[11]

OBJECTIVE: SEQUENTIALLY MANEUVER REACTOR MODULES (incrementally if in parallel) TO STABLE OPERATING CONDITIONS.

(underlined items below are operator permissives required to continue automatically.)

- o CONFIRM AUXILIARY SYSTEMS IN SERVICE AND INITIAL CONDITIONS MET (pressurization, etc.)
- o REQUEST MODULE STARTUP
- o MONITOR SUBCRITICALITY TESTS AND CONDITIONS
- o INDICATE ACHIEVEMENT OF CRITICALITY TO OPERATOR
- o ASCERTAIN PROPER FEEDWATER CHEMISTRY
- o REQUEST MODULE STEAM PRODUCTION
- o CONFIRM ESTABLISHMENT OF REQUIRED MODULE STEAM AND MAIN STEAM HEADER CONDITIONS (e.g., pressure, temperature, etc.) FOR MODULE HEADERING
- o REQUEST CONNECTION TO MAIN STEAM HEADER AND INCREASE MAIN STEAM LOAD INDEX
- o REQUEST ESTABLISHMENT OF TURBINE SEALS, CONDENSER VACUUM AND TURNING GEAR OPERATION

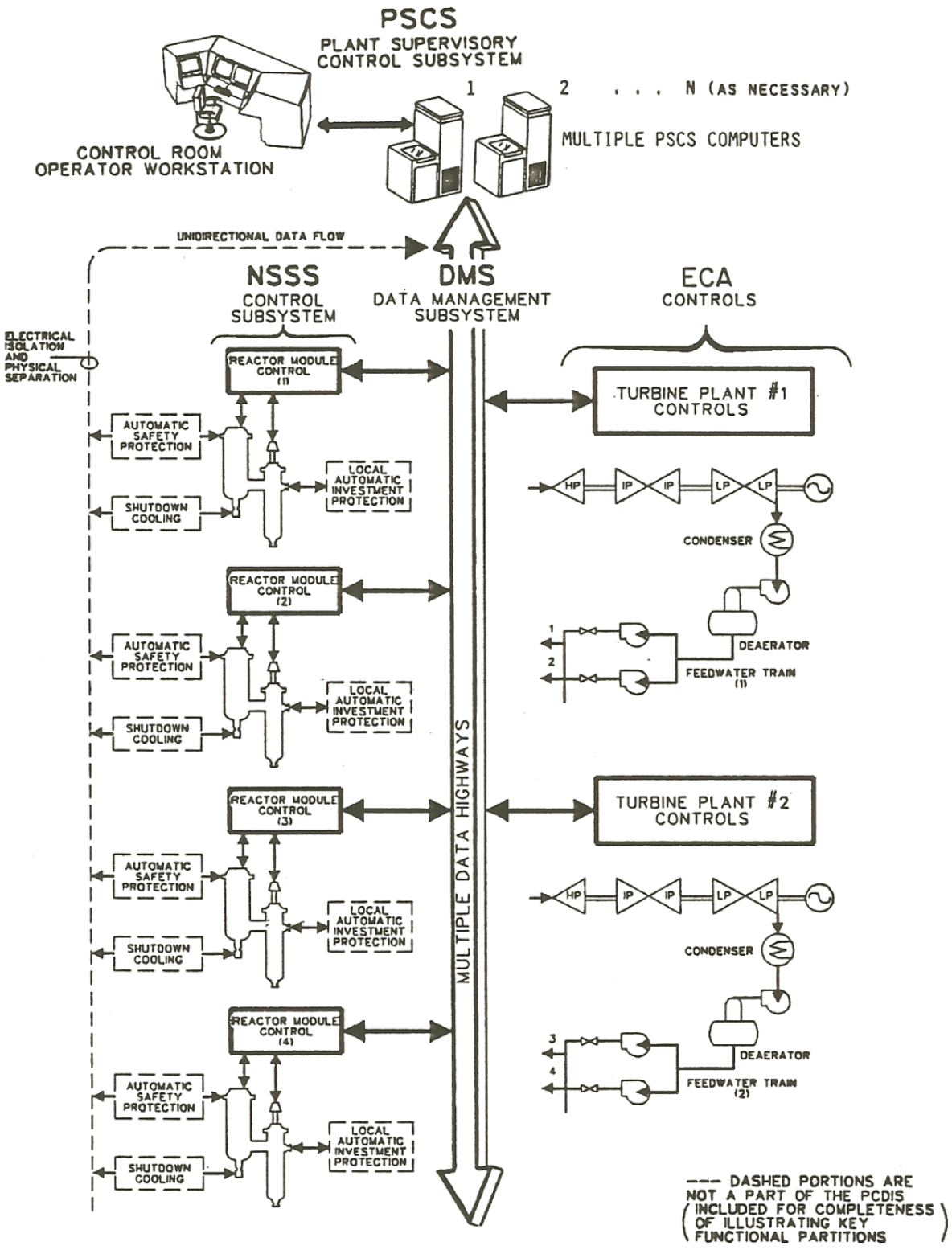

Fig. 4. MHTGR plant supervisory control subsystem overview.[11]

2.1.11.5.2 PSCS startup/shutdown

Table 3 summarizes the PSCS control strategy during plant startup and shutdown. Reactor module startup from depressurized shutdown consists of bringing the modules up to minimum stable operating conditions sequentially through a series of operator checkpoints several times during the startup. These checkpoints are underlined in the table.

Load levels for the modules are raised in parallel to a common average level at ramp rates of +0.5% per minute. Modules are connected to the main steam header one at a time. The logic for shutdowns is the reverse of startups. For shutdowns, the modules are shut down in a parallel manner at incremental levels. Modules are disconnected from the main steam header one at a time.

Table 3. PCSC control strategy for normal startup or shutdown[11]

OBJECTIVE: SEQUENTIALLY MANEUVER REACTOR MODULES (incrementally if in parallel) TO STABLE OPERATING CONDITIONS.

(underlined items below are operator permissives required to continue automatically.)

- o CONFIRM AUXILIARY SYSTEMS IN SERVICE AND INITIAL CONDITIONS MET (pressurization, etc.)
- o REQUEST MODULE STARTUP
- o MONITOR SUBCRITICALITY TESTS AND CONDITIONS
- o INDICATE ACHIEVEMENT OF CRITICALITY TO OPERATOR
- o ASCERTAIN PROPER FEEDWATER CHEMISTRY
- o REQUEST MODULE STEAM PRODUCTION
- o CONFIRM ESTABLISHMENT OF REQUIRED MODULE STEAM AND MAIN STEAM HEADER CONDITIONS (e.g., pressure, temperature, etc.) FOR MODULE HEADERING
- o REQUEST CONNECTION TO MAIN STEAM HEADER AND INCREASE MAIN STEAM LOAD INDEX
- o REQUEST ESTABLISHMENT OF TURBINE SEALS, CONDENSER VACUUM AND TURNING GEAR OPERATION

2.1.11.5.3 PSCS normal operation

Table 4 summarizes the MHTGR's PSCS control strategy during normal plant power generation (25–100% load). The primary control function is to allocate main steam flow (secondary side) demands and feedwater flow (primary side) demands to the energy conversion area and nuclear steam supply control subsystems, respectively. The PSCS calculates the main steam demand equivalent of the generator electrical demand from which an algorithm calculates feedwater demand. These are continuously apportioned equally among the available turbine generators and reactor modules through another algorithm.

2.1.11.5.4 PSCS refueling

The PSCS does not perform any refueling control functions. Control room operator-initiated functions that could add positive reactivity to a shutdown module are deactivated.

Table 4. PCSC control strategy for normal operation[11]

OBJECTIVE: MANEUVER ALL MODULES IN PARALLEL FROM 25 PERCENT TO 100 PERCENT RATED LOAD AFTER OPERATOR PERMISSIVES ARE ACKNOWLEDGED. STRATEGY: o CONVERT PLANT OUTPUT DEMAND (MWe or percent capacity) INTO TOTAL FEEDWATER AND MAIN STEAM DEMANDS o DETERMINE LOAD DEMANDS AND RATES OF LOAD CHANGE RELATIVE TO design rated plant capacity if all modules are unconstrained available plant capacity if any modules are constrained o EQUALLY ALLOCATE INDIVIDUAL REACTOR MODULE FEEDWATER AND MAIN STEAM ADMISSION DEMANDS (FOR AVAILABLE REACTOR MODULES AND T-G's) o IF - ANY MODULES ARE CONSTRAINED and IF - THE PLANT LOAD CHANGE RATE REQUIRES MODULE LOAD CHANGES AT RATES EXCEEDING THOSE USED TO MEET 15 PERCENT STEP LOAD INCREASES THEN - DECREASE THE PLANT LOAD CHANGE RATE TO THAT RATE ACHIEVABLE BY THE UNCONSTRAINED MODULES

2.1.11.5.5 Shutdown

The PSCS primarily performs monitoring functions for portions of the plant that are shut down to ensure that the reactor is maintained in a shutdown condition, core geometry is maintained, neutronic measurements are acceptable, and decay heat removal functions are provided.

2.1.11.5.6 PSCS abnormal operating modes

Table 5 summarizes the PSCS control strategy during abnormal power generation during which the PSCS coordinates continuous plant operation during and following transient conditions associated with problems with major reactor module or turbine generator systems or components. The PSCS implement control strategies for reloading the plant once problems have been corrected. The PSCS is capable of recovering from generator load rejects and turbine trips (except on low condenser vacuum) from any power level without requiring a reactor trip, even if reactor modules or turbine generators are constrained for some reason.

Table 5. PCSC control strategy for MHTGR abnormal operation[11]

OBJECTIVE:		MAINTAIN POWER GENERATION UNLESS INVESTMENT PROTECTION IS CHALLENGED OR COMPROMISED.
STRATEGY:		
o	IF	- REACTOR POWER IS GREATER THAN HEAT SINK CAPABILITY (e.g., turbine trip, feedwater reduction, etc.)
	THEN	- INITIALLY DECREASE REACTOR MODULE LOAD INDEX TO ACHIEVE AN AUTOMATIC LOAD RUNBACK
	AND	- FOR A TURBINE TRIP, EVENTUALLY INCREASE ALL LOAD INDICES IF AT LEAST ONE TURBINE IS AVAILABLE
o	IF	- REACTOR POWER IS LESS THAN HEAT SINK CAPABILITY (e.g., module trip, etc.)
	THEN	- ASCERTAIN PLANT ABILITY TO MAINTAIN THE ORIGINAL PLANT OUTPUT
	AND	- EVENTUALLY INCREASE REACTOR MODULE LOAD INDICES TO COMPENSATE FOR REDUCED PLANT OUTPUT
	OTHERWISE	- REDUCE TURBINE LOAD INDEX TO ACHIEVE AN AUTOMATIC LOAD RUNBACK

2.1.11.6 Nuclear steam supply system control subsystem

Each MHTGR reactor module has its own nuclear steam supply system (NSSS) control subsystem that controls reactor conditions and the supply of steam to the main steam header. The NSSS control subsystem responds to demands from the PSCS and then controls its feedwater flow demand (primary system demand) to meet its load demand. The NSSS control subsystem performs its function by

1. following the mission set by the PSCS (with plant operator concurrence), including startups and shutdowns;
2. monitoring conditions required for the NSSS to be operable;
3. determining the strategy to be used to produce the module's steam requirements;
4. implementing the chosen control strategy; and
5. displaying information on the NSSS status and conditions.

The major functions of the NSSS control subsystem are to manage module feedwater flow control demand, circulator speed control, power characterization, main steam temperature control, and main steam pressure during startup. The NSSS control subsystem reactor module control loops are configured to accommodate feedwater, reactor module, and turbine trips. In addition, the control loops minimize transient extremes to protect plant equipment and optimize NSSS availability.

NSSS feedback control algorithms are proportional plus integral plus derivative expressions (PID) or proportional plus derivative (PD). The result of this feedback algorithm may be summed with a feed forward signal that is a function of the reactor module load setpoint. The sum of the compensation output and the feed forward signal is passed through limiter logic to provide high, low, and/or rate limits. The output from the limiter is sent to the manipulated variable (dependent variable). If at a limit, a signal is sent to the PID to force it to track such that the sum of the compensation output and the feed forward satisfy the limit condition. A number of special control schemes were devised for specific situations. The special controls schemes altered the normal settings for ramp rates, feedback gains, etc., to improve system response in the special event. The complexity of these system and potential for unintended functions were not analyzed.

The NSSS control subsystem provides startup/shutdown, normal operation, refueling, shutdown, and abnormal operation functions.

2.1.11.6.1 NSSS startup/shutdown

The MHTGR's startup/shutdown covers operating conditions in the 0–25% module load range. The NSSS control system has the capability of allowing the hot water and steam from startup and shutdown operations to bypass the main turbines and pass to a flash tank. Each module has its own bypass. While in startup or shutdown, the module main steam isolation check valve is closed so that other modules may continue to operate.

Hot water and steam temperatures range from 27°C (liquid) to 541°C (superheated steam) by the NSSS control subsystem control of reactor power and circulator speed. Once at temperature, the pressure is raised slightly above the main steam header pressure through a slow closure of the bypass valve and a slow opening of the isolation check valve.

Special NSSS control loop gains are used during startup and shutdown to allow automatic control with outlet steam conditions below rated values and feedwater flow less than 25%. Automatic control is maintained during final stages of steam generator and turbine warmup during startup and in the initial stage of steam generator cooldown during shutdown. Except for certain safety checks, operation is fully automated.

2.1.11.6.2 NSSS normal operation

Main steam header pressure response is fast relative to reactor module thermal response during normal operation, so that pressure changes are typically small. Because of the main steam header pressure controller compensation speed, pressure response is largely decoupled from steam temperature in transient conditions. Main steam temperature is controlled by manipulating reactor power and circulator speed. Even in large load changes, main steam temperature deviations are negligible an hour later.

2.1.11.7 Energy conversion area control subsystem

The energy conversion area control subsystem provides monitoring and control for electrical power generation. The data management subsystem provides the data communication between the subsystems.

The plant control systems are to provide complete, computerized, automatic control of the plant using hardware platforms characterized as redundant and fault tolerant.

The NRC staff voiced several concerns during their review of the preapplication safety information document, which was to be examined in more detail upon submission of the real application. These included (1) the interconnected control of the four reactor modules and two turbine generators, since this is a configuration new to the industry with the goal of maintaining some power production even with the shutdown of a reactor module or a turbine generator; (2) isolation between the normal plant control system and the safety-related plant protection and instrumentation system; and (3) failures of the nonsafety control systems that put the plant outside of event category II sequences. The NRC staff concluded that the design could be implemented in an acceptable manner.[12]

2.1.11.8 Miscellaneous control and instrumentation group

The miscellaneous control and instrumentation group systems provide additional data to the operator and retention in the archives. These systems are (1) the NSSS analytical instrumentation system; (2) radiation monitoring system; (3) seismic monitoring system; (4) meteorological monitoring system; and (5) the first detection and alarm system. The NRC concluded that further review of these nonsafety-related systems was not needed for the pre-application design review stage.

2.2 SAFETY EVALUATION

The MHTGR was designed to be a safe, economical plant that follows principles of defense-in-depth in meeting requirements from its plant owners and the regulator. The discussion that follows is summarized from the applicants' assessments as described in the *Conceptual Design Summary Report, Modular HTGR Plant, Reference Modular High-temperature Gas-cooled Reactor Plant.*[13] The function of protection systems in the safety evaluation is discussed.

The following four goals of the plant design were established:

- Goal 1: maintain safe plant operations,
- Goal 2: maintain plant protection,
- Goal 3: maintain control of radionuclide release, and
- Goal 4: maintain emergency preparedness.

In recent history, other gas-cooled reactors have been successful in complying with NRC requirements for Goals 1 and 2. The applicant noted that the MHTGR was also designed to use similar high-quality fuel so that radionuclide release probabilities and amounts are low during normal operation or accident situations. To accomplish Goal 3, radionuclides are to be retained within the fuel with high confidence and with minimal reliance on active safety systems or operator actions. This is to be accomplished by the specification of the size of the reactor core, its shape, and power density. The vessel type also plays a principal role in the elimination of active systems to remove decay heat under both pressurized and depressurized conditions. The particle fuel coatings also effectively retain fission products under a wide range of accident conditions, serving as the primary containment boundary for fission products. Thus, assurance of safety is based on assurance of fuel particle integrity. If this is proven, secondary mitigation measures or barriers are not necessary under normal or accident conditions. That is, ensuring the integrity of the fuel particles ensures that safety criteria are met and can reduce the requirements normally associated with Goal 4.

The MHTGR report includes analysis of structures and components for an operating basis earthquake of 0.15 g and a safe shutdown earthquake of 0.3 g for a range of soil types varying from uniform rock with a high shear wave velocity, soft soil with a low shear wave velocity, to a varying condition with softer soil at the surface and harder soil below. Site-specific analyses will be required but are expected to be bounded by the conditions above. Effects on the reactor silo and vessel system, reactor core and core supports, and RCCS structures and components were assessed, and the plant was concluded to possess adequate seismic capability down to an event frequency of 5×10^{-7} per year.

The MHTGR has been analyzed to ensure the adequacy of the design to control accidental radionuclide releases to within the limits of regulatory criteria, including the Environmental Protection Agency (EPA) Protective Action Guide (PAG) limits. Design basis events (DBEs) were specified and evaluated that considered the mechanistic response of the plant. These serious, but rare, events might be expected over the lifetimes of several hundred like plants but would be highly unlikely at any one plant. Nonmechanistic responses known as safety-related design conditions (SRDCs) are also considered in which DBEs are analyzed without taking mitigating effects of nonsafety-related types into account.

The safety performance of the MHTGR is based on the ability of trilayer isotropic (TRISO) ceramic coated-particle fuel to effectively retain fission products. This is ensured if functions to control heat generation, remove core heat, and protect against chemical attack of the fuel are maintained during normal operation and under transient conditions represented by DBEs and SRDCs.

2.2.1 Control of Heat Generation Events

The ability to control heat generation was evaluated through two events: (1) loss of normal cooling from the heat transport system with a failure to scram and (2) unplanned control rod withdrawal of an outer reflector control rod group of three rods.

For the loss of normal cooling event, the core temperature rises, which causes the reactor to go subcritical due to the negative fuel temperature coefficient. Core power drops to about 33% in less than 1 minute. The reserve shutdown system actuates after about 56 seconds due to core power/circulator speed ratio exceeding its trip point for 50 seconds. The reserve shutdown system quickly reduces core power to decay heat levels. With no forced circulation, decay heat causes core temperatures to rise to a peak maximum temperature of 1296°C after almost 4 days. System pressure peaks at about 1009 psia, which is below the actuation pressure for the pressure relief system. In this example, the pressure boundary integrity is retained, temperatures are below the onset of fuel particle failure, and no radionuclides are released.

For the unplanned control rod withdrawal, core power increases and core temperature rises. The negative fuel temperature coefficient counteracts the reactivity increase from the rod withdrawal. A reactor trip occurs after about 99 seconds on high core power/flow ratio and outer rods drop. Peak core power is about 147% at about 100 seconds. During this excursion, fuel temperature peaks at about 1394°C, which is below the threshold of fuel damage. There are no radionuclide releases.

2.2.2 Control of Core Heat Removal Events

A depressurization accident is the limiting event for challenging the ability to remove core heat. A helium leak from a 12.7 $in.^2$ hole located at the top of the steam generator vessel, corresponding to a pressure relief train opening, is assumed. The primary system depressurizes in minutes. After about 20 seconds, a reactor trip signal is received on low pressure. The nonsafety-related shutdown cooling system is assumed to fail. Heat is removed from the core by radiation and conduction to the reactor vessel and from there by radiation and convection to the RCCS panels and from there to the environs via natural circulation. This is an entirely passive cooling process. No systems actively operate or change state.

Because of the thermal inertia of the core, maximum core temperatures occur after about 80 hours. Figure 5 shows the effect of this transient on core temperatures. The maximum fuel particle temperature is just over 1600°C. After about 80 hours, the core heat removal exceeds the core heat generation and the reactor core begins cooling. Fuel particle temperatures remain below the point at which gross failure of the silicon carbine layer occurs; however, some fuel particle failure is expected above 1600°C. For this example, there is a loss of the primary system pressure boundary and leakage of fission products to the reactor building and the environs. Approximately 160 curies of ^{131}I, the limiting radionuclide, is assumed to be released from the core, with approximately 26 curies released to the reactor building. Of that, approximately 1 curie would be released to the environment. The cumulative offsite dose to the thyroid of a person at the exclusion area boundary of the plant is estimated to be 0.36 rem at 30 days. (The 10 CFR 100 limit is 300 rem; the PAG limit is 5 rem.)

2.2.3 Control of Chemical Attack Events

The limiting event for controlling chemical attack is a depressurized conduction cooldown with moisture ingress. This could occur if a steam generator tube ruptures. After the tube rupture, a high-power/flow ratio limit is exceeded as a result of a power increase resulting from the moisture entering the core, which causes a reactor trip. The nonsafety-related moisture monitoring system is assumed to fail. Primary system pressure increases, and a reserve shutdown system actuation occurs on high pressure. The nonsafety-related shutdown cooling system is assumed to fail. The main coolant system and the steam generator isolate automatically; however, the steam generator dump system is assumed to fail, which provides a source of about 9000 lbm of steam to the primary system.[13] The heatup of moisture in the primary system in the core causes primary system pressure to increase, which activates the pressure relief

system about 6 minutes into the accident. The relief valve is assumed to cycle once or twice and then fail open, resulting in a depressurized system.

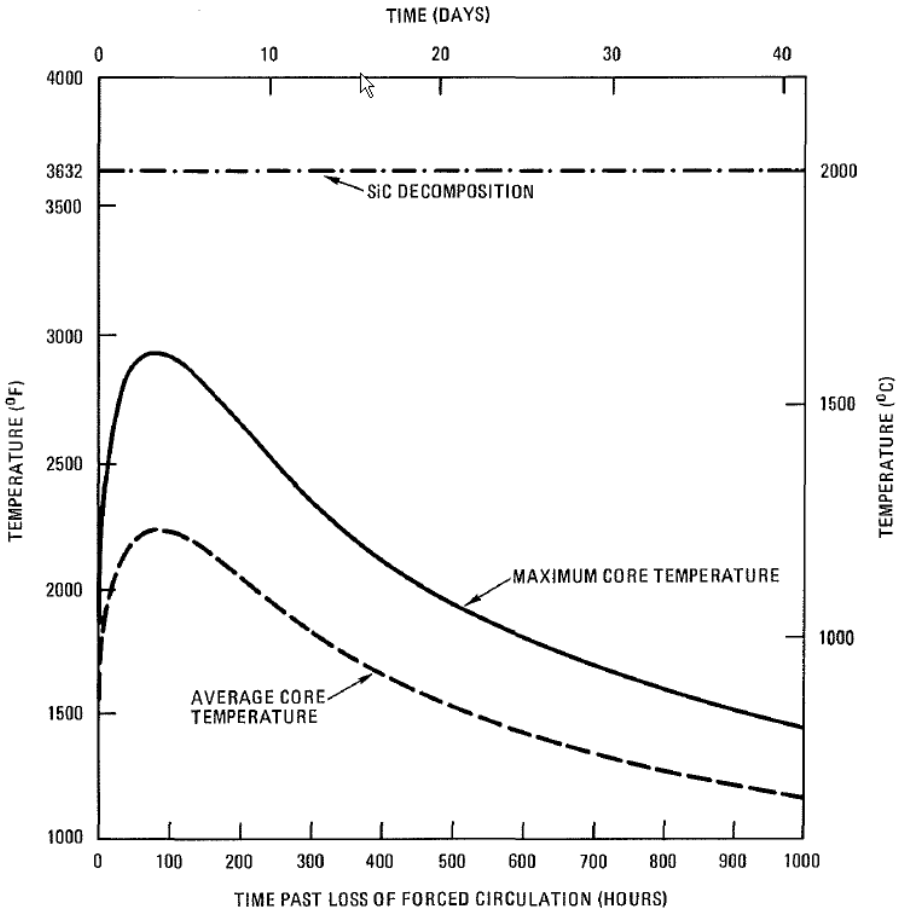

Fig. 5. MHTGR core temperatures during depressurized conduction cooldown.[13]

The graphite core components, including the fuel, are subject to chemical attack from the moisture. This occurs mostly in the hotter lower sections of the core; however, oxidation is not expected to be enough to create concerns with structural integrity. Some fission products are expected to be released from fuel particles that have defective coatings and undergo hydrolysis. Fission product release is also expected due to coating degradation from high temperatures. The fission products migrate to the reactor building and environs. Iodine-131 is again the limiting radionuclide. In this accident, about 50 curies is estimated to be released to the reactor building and about 5 curies is expected to be released to the environment. The cumulative offsite dose to the thyroid of a person at the exclusion area boundary of the plant is estimated to be 4.8 rem at 30 days. (The 10 CFR 100 limit is 300 rem; the PAG limit is 5 rem.)

2.2.4 Probabilistic Risk Assessment (PRA)

A PRA of the MHTGR was conducted by General Atomics Technologies.[14] The applicant stated that the expected reactor behavior is “extraordinarily benign,” with limited offsite releases predicted even for extremely unlikely accidents. The design met risk limits of NRC safety goals with substantial margin. The design met user requirements “of no need for public sheltering or evacuation based on the (PAG) does for emergency planning.” Accident frequencies greater than 10^{-7} per year were considered. External events

such as loss of offsite power and earthquakes that could affect multiple plant systems were included in the PRA. The methodology included initiating event selection, event trees, fault trees, common mode failures, transient radionuclide transport and dose, and uncertainty analysis.

The PRA indicated that the overall safety of the MHTGR, which relies on passive features and high integrity fuel, is not dependent on active systems and operator responses. The applicant noted that "no accident scenarios of meaningful probability were identified that could compromise the fuel and lead [to] gross releases." Radionuclide releases in all cases stemmed from manufacturing defects in the fuel made apparent in stresses during accident conditions. Studies indicated that an accidental release resulting in a whole body gamma dose at the exclusion area boundary above the 1 rem PAG limit is a rare occurrence with an expected frequency less than 5×10^{-7} per year. For the thyroid, the dose is expected to be less than the 5 rem PAG limit, a rare occurrence with about the same frequency.

2.3 KEY CONTROL AND PROTECTION DESIGN METHOD ISSUES FOR NGNP

2.3.1 Issues in Protection Systems

The inherent safety properties of HTGRs eliminate or significantly reduce the risk of some of the most severe accidents that LWRs must address. However, some new types of active safety systems may require formulation of new requirements and guidance. For example, water ingress accidents (such as from steam generator tube ruptures) can result in significant amounts of water (steam) entering the core that could cause increases in reactivity and system pressure, fuel hydrolysis, formation of water gas, and oxidation of core graphite. Mitigating actions for these events include a reactor scram, a loop trip (i.e., a circulator trip and steam generator isolation), and a steam generator dump.

For air ingress accidents (following a depressurization), the primary objective would be to limit the long-term supply of oxygen (fresh air) in the confinement building that could eventually enter the primary system. Natural convection ingress flow rates are usually limited to relatively low values due to the high core flow resistances and resistances in other parts of the flow paths. Typical scoping calculations of air ingress accidents indicate that although the oxidation rates for reactor-grade graphite are quite low, the oxygen in the entering gas is typically completely consumed, generating heat and forming CO_2, well before it exits the core. In fact, at least for the first several days of significant air ingress, analyses show it to be mostly consumed in the lower support blocks and lower reflector, with relatively little oxygen reaching the active core. Of the many ad hoc possibilities for air ingress accident mitigation, those that limit the available oxygen in the confinement building near the point of ingress are the most beneficial, such as sealing off the offending compartment or injecting inert gasses.

2.3.2 Issues in Control Systems

2.3.2.1 Advanced control design methods

The NGNP can be expected to make extensive use of digital technology and may employ advanced control design methods to optimize performance. In addition, it will likely have a much higher level of automation than existing plants and may employ modern control methods to provide advanced functions such as trip avoidance strategies to reduce the demands on the protection system. A primary safety-related concern for advanced, highly integrated control systems is the potential that the plant may operate or fail in a way that results in transients that are not bounded by the plant safety analysis. Another key concern is that failure of complex control systems could inhibit the successful execution of required safety functions.

The inherent safety characteristics (e.g., large thermal mass of moderator and fuel for slow heatup rates, a large negative temperature coefficient, inert gas coolant, ceramic fuel particle coatings that can withstand very high temperature without releasing fission products, a passive heat removal capability) of the HTGR designs proposed for NGNP may address the first concern by limiting the potential impact of control

system inadequacy or failure as a consequence of the plant design. This determination depends on the results of the plant accident and transient analyses and the demonstrated fidelity of those findings.

Regarding the concern about the impact of the control system on the safety system, adherence with the independence requirements of IEEE 603-1991 generally provides the key basis for ensuring that the integrity of safety functions is adequately protected. Given the digital capacity to enable greater interconnection and integration among systems, additional guidance on issues such as communications independence and command prioritization has been provided by NRC through the interim staff guidance for digital I&C. If, as is the case for the ALWR designs, the NGNP automated control room maintains adequate independence between the control and safety systems, then the impact of automation will primarily involve operational control functions so the necessary assurance of adequate safety can be established based on the safety system implementation. Consequently, the assessment of the adherence to safety system requirements, in particular the independence criterion, will be a crucial aspect of any regulatory review for the highly automated control room of the NGNP.

Issues associated with automation in highly integrated control rooms are discussed in detail by Wood et al. (last of the four reports listed in Section 1). In addition, the impact of unique concepts of operation, such as multiunit control and coupled nuclear and industrial process control, are also presented in the Task 2 report.

2.3.2.2 Support system controls

The discussion in this report focuses on the protection and control design methods for the reactor and major heat transport systems. Other controls may eventually need to be examined further depending on as of yet unavailable design details. Some control systems in HGTRs may be new or unique and may have greater safety implications than control in traditional LWR power plants. Two such control systems which may need further examination are the magnetic bearing control for the helium circulator and shaft seal controls.

One potential concern regarding the magnetic bearing controller is that a failure of the control device and catcher bearings could cause the displacement of the impeller and motor shaft leading to failure of the pressure boundary in the circulator. The magnetic bearing control design issue has been raised as a part of this review but no details of the magnetic bearing controls and their safety implications in plants which employ them have been found in literature. This event, a control system failure leading directly to a loss of coolant accident, is a possible accident with a much higher severity category than other control system failures in licensing reviews.

A related problem is helium shaft seals. The helium circulator motor and shaft are likely to be externally sealed. That is, the motor and impeller are sealed within the helium pressure boundary. However, the main coolant cannot be allowed to circulate freely around the motor and impeller because of dust in the coolant which could damage the circulator components and radioactive contamination deposits which would greatly increase the radiation exposure of workers during maintenance. The helium from the main reactor circuit must be kept out of the internal motor and impeller space by internal seals and a flow of higher pressure clean helium into the space toward the reactor. Because the consequences of failure are severe, control of the seal flow and cooling becomes an issue from a regulatory perspective.

2.3.3 System Classification

In the preliminary licensing proposal on the MHTGR presented by General Atomics to the NRC,[15] a licensing strategy was proposed to take advantage of the inherent safety of the HTGR and reduce the number of systems considered to perform safety-related functions. In this approach, certain functions that protect equipment but are not necessary for satisfying regulatory dose limits in accident analyses are designated as “investment protection systems” rather than “safety-related systems.”

The inherent safety function of HTGRs provides only limited protection of equipment other than the fuel itself. While the fuel is generally protected and radiation release is predicted to be within 10 CFR 100 limits when relying solely on passive response of the reactor system, other equipment important to investment and operation may be vulnerable at the temperatures that may exist in the reactor and confinement cavity when only the inherent passive cooling is available. Active components such as pumps, valves, motors, control rod drives, and instrumentation may in fact be damaged by the high temperatures reached when the plant is involved in a worst case event unless active cooling systems are operational. The class of support function that would cool the active components is what would be designated as investment protection.

The concept of investment protection as an intermediate class between safety-related and nonsafety-related is a licensing approach that has not been previously approved by the NRC. When the MHGTR pre-conceptual design was reviewed by the NRC, one of the unresolved issues was the concept of "investment protection" rather than "safety-related" designation for equipment analogous to LWR systems which are safety grade.

As for every reactor design, the determination of whether I&C functions should be considered as control or protection will depend on the results of transient and accident analyses for NGNP. Clearly, safety functions and their corresponding protective actions must be treated in accordance to safety system design requirements. The remaining control functions are designated according to the safety/nonsafety classification based on the determination of whether, through normal operation, system failure or inadvertent operation, they can affect the performance of critical safety functions. Thus, the treatment of the systems that perform these functions is dependent on analysis of the impact of these systems on the execution of safety functions. If the investment protection system of the NGNP is determined to be a nonsafety system, it still may be required to demonstrate augmented quality, following the guidance of Digital I&C ISG-02. This would be the case if it is allocated a role as a diverse means of performing an equivalent safety function in the event that a common-cause failure (CCF) disables protection afforded by another echelon of defense.

Nonsafety systems that are relied on for beyond design basis events to reduce core damage frequency below 10^{-4}/reactor year are treated under special requirements called "regulatory treatment of nonsafety systems" or RTNSS.

2.4 KEY ISSUES FOR HIGHLY AUTOMATED CONTROL ROOM DESIGNS IN VHTRS

The control room and the underlying levels of automation provided by the I&C systems of a VHTR plant may be significantly different from conventional LWRs because of the inherent safety features of HTGRs and the capabilities available through extensive use of digital technology. Experience in existing plants (both LWR and HTGR) has ranged from collections of analog single loop control and hardwired simple displays to integrated digital control and flexible, multiscreen video displays. Operational approaches have progressed from primarily manual operation to system-based automation with strategic coordination by the operations staff. Operators have transitioned from active participants in routine operational actions to supervisors of automatic control systems with responsibility for intervention under abnormal circumstances. The designs for ALWRs, such as the Westinghouse AP1000, the Mitsubishi APWR, AREVA EPR, and the GE–Hitachi ESBWR, employ more fully digital I&C systems within an integrated, layered communications architecture to support more highly automated management of a single reactor unit throughout the range of normal operational modes. Nevertheless, ALWR design have thus far adopted architectural approaches to implementing I&C functions that are fundamentally the same as for operating plants, building on the experience gained over the years. The control rooms for next generation reactor designs are expected to be similar to those emerging for modernized plants and ALWR designs. However, some next generation concepts envision multiple modules controlled from a single integrated,

highly automated control room. The transition to highly integrated, fully automated control rooms poses technical issues that must be considered to ensure appropriate coverage in a regulatory review.

2.4.1 Automation

Highly automated intelligent control involves more than simple automation of routine functions. It includes the detection of conditions and events, determination of appropriate response based on situational awareness, adaptation to unanticipated events or degraded/failed components, and adjustment of operational goals. To facilitate optimal plant operations without excessively burdening the plant operational staff, a highly automated control system provides the capability to accomplish higher level supervisory and decision functions. The automation and intelligence incorporated in a highly automated control system can range from automated control systems that perform simple transition among predefined operational strategies and functional configurations based on detection of triggering events, to nearly autonomous control systems that can independently perform control, detection, decision, reconfiguration, and even self-maintenance, based on human permissives.

The design details for the control room of the NGNP and its underlying I&C systems have not yet been established. The main I&C systems that have been identified for the NGNP are dedicated to the following primary functions: reactor protection (safety), investment protection (limitation), and plant control. In the case of the one conceptual design that is actively being developed under the program, the design foundation for the plant control and protection architecture is drawn from the past development by General Atomics for the GT-MHR and New Production Reactor (NPR), which are based on a design philosophy heritage with roots in the early 1990s. Experience with automation in past and current HTGRs is limited to direct automation of simple control loops with some instances of supervisory control and/or feedforward action to coordinate controller action. The design concept for the MHTGR provides for multi-module operation with supervisory control for demand allocation at the highest level and automatic operational control at the individual module level. In each implemented and conceptualized design, separation and independence are maintained between the automatic control and protection systems.

The emphasis on a commercial plant development strategy for the NGNP program provides an impetus to employ mature technologies; consequently, there is a reasonable expectation that the NGNP will adopt an automation approach similar to that employed by ALWRs. Thus, the NGNP can be expected to make extensive use of digital technology to provide for plant-wide integrated access to data, coordination among individual automatic control loops, and condition monitoring and other computerized operator support tools. The highly integrated control rooms of ALWR designs have been addressed through clarified regulatory guidance on acceptable means for satisfying regulations. The primary safety-related concern for control systems are the potential that they may operate or fail in a way that results in transients that are not bounded by the plant safety analysis or inhibits the successful execution of required safety functions. The inherent safety characteristics (e.g., a small operational excess reactivity, large thermal mass of moderator and fuel for slow heatup rates, a large negative temperature coefficient, inert gas coolant, ceramic fuel particle coatings that can withstand very high temperature without releasing fission products, a passive heat removal capability) of the HTGR designs proposed for NGNP may address the first concern by limiting the potential impact of control system inadequacy or failure as a consequence of the plant design. This determination depends on the results of the plant accident and transient analyses and the demonstrated fidelity of those findings. Regarding the concern about the impact of the control system on the safety system, adherence with the independence requirements of IEEE 603-1991 generally provides the key basis for ensuring that the integrity of safety functions is adequately protected. Given the digital capacity to enable greater interconnection and integration among systems, additional guidance on issues such as communications independence and command prioritization has been provided by NRC through the interim staff guidance for digital I&C. If, as is the case for the ALWR designs, the NGNP automated control room maintains adequate independence between the control and safety systems, then the impact of automation will primarily involve operational control functions so the

necessary assurance of adequate safety can be established based on the safety system implementation. Consequently, the assessment of the adherence to safety system requirements, in particular the independence criterion, will be a crucial aspect of any regulatory review for the highly automated control room of the NGNP.

It is possible that the NGNP will seek to extend the degree of automation beyond the current state-of-the-practice in the nuclear power industry by incorporating more advanced characteristics to provide for optimal operation of the plant, whether as a single unit coupled with flexible energy conversion options or as multiple units serving several customers (e.g., electric grid, industrial process heat users). In addition to the digital I&C capabilities common to ALWR designs, the resilient design features investigated under the NGNP program and the autonomous control concepts considered for space nuclear power systems offer the opportunity for greatly enhanced operational efficiency, reduced reliance on direct intervention by operators for normal and off-normal operations, and embedded capital investment protection for key equipment, systems, and structures. The characteristics that distinguish resilient and autonomous control from the more conventional control strategies employed in the nuclear power industry are the capabilities to anticipate, decide, and adapt to conditions and events. These characteristics may introduce regulatory issues that have not been posed by ALWR automation approaches.

Given the immaturity of the technologies in the nuclear application domain, it is not expected that a comprehensive resilient or autonomous control system will be developed in the near term. However, it should be anticipated that resilient and/or autonomous features would be incorporated in the NGNP highly automated control system design to enhance performance and dependability (e.g., reliability, fault tolerance, flexibility). Many of these features emphasize reliability, optimization, and adaptation, which may not necessarily be completely consistent with the primary goal of safety. As discussed above, if these features are limited to the control system and it can be shown that adequate independence exists between the safety and control systems, then the associated regulatory issues should be manageable within the existing regulatory framework.

The Idaho National Laboratory (INL) investigation of a resilient control strategy for NGNP identified several notional scenarios in which local control autonomy within an adaptive, intelligent architectural approach can provide an effective capability to mitigate the impact of threats, events, and degraded conditions. The scenarios illustrate some of resilient features that may not be desirable for safety systems. In the scenario involving undetected changes to sensors, an identified adaptive response involves substitution of the invalid signals by inferred parameters based on other validated measurements and operational models. The scenario regarding inference of unmeasured parameters includes prospective adaption of control based on changes to control settings (e.g., set points, controller gains, rate limits) to optimize performance based on inferred conditions. For the situation where end-use transients might induce operational upsets, forms of adaptation could involve switching among alternate operational schemes (e.g., changing control goals in real time). The scenario related to a cyber threat identified substitution of validated signals for suspect data or switching to unaffected control algorithms (i.e., algorithms based on different signals) as means of adaptation to thwart an attack. It was also noted in discussing the cyber attack scenario that randomization of communications traffic could serve as a defensive measure to minimize vulnerability to attack. The adaptive actions identified in the notional scenarios could pose safety concerns unless it can be shown that the adaptation would not inhibit the execution of the safety function or compromise adherence to regulatory requirements (e.g., independence, integrity). The suggested cyber defense approach of randomized communications characteristics could run counter to desired safety characteristics such as deterministic, predictable performance. Safety system implementations employing similar adaptive resilient features would require very careful assessment to ensure that the capability to execute safety functions is not compromised.

The safety evaluation of the safety system modernization at the Oconee Nuclear Station serves an example of recent regulatory experience with the introduction of limited resilient features in digital safety applications.[16] In the digital safety system at Oconee, signal validation functions are implemented in each

safety channel to provide additional fault tolerance against signal failure, beyond the traditional use of redundancy in system design. To support the signal validation capability, interchannel communications is provided among the redundant channels to share signals for comparison. The implementation posed a challenging review to ensure that the independence criterion was not violated. The guidance of ISG-04 was employed to support the safety findings. It was claimed that the signal validation capability enhances the performance of the safety function. However, based on its analysis, the NRC staff determined that, while the signal validation provides additional demonstration of reliability, those "features are not necessary to perform the safety function, nor do they support or enhance the safety function." Therefore, the interchannel communications did not satisfy the ISG-04 Staff Position 1, Point 3, in that its purpose is to support the performance of function that is not directly related to the safety function. As a result of this determination, a very detailed evaluation of the impact of the communications on the safety function was necessary. Briefly, the findings were that, in the presence of communications failure, the signal validation algorithm provides for progressive degradation to an acceptable state. Failure of all of the communications links would ultimately result in the affected channel(s) performing their safety function based on the sensor input specific to that channel. The staff determined that, for this particular implementation, performance of the safety function was not dependent on external communications nor would the safety function be impaired by this communications. As a result of this very detailed review, the staff concluded that the interchannel communications and the signal validation it supports are acceptable in this instance. Similar detailed reviews will likely be necessary to assess the impact of any nontraditional resilient features (or the failure of those features) that may be incorporated in safety systems within a highly automated control room design.

2.4.2 Limitation vs Safety

Most LWRs contain some limitation functions and control interlocks as elements of the automated control system. Effectively, these functions enable trip avoidance to promote availability or provide mechanisms to ensure investment protection. With a separate, safety-related RLS, German nuclear power plants demonstrate the most extensive and formalized use of limitation functions within the defense-in-depth hierarchy of nuclear power plant I&C architectures. These functions, and the control or limitation systems that implement them, are intended to complement the reactor protection system by providing intermediate response to abnormal conditions and thereby avoid challenging the safety system.

In the preliminary licensing proposal on the MHTGR presented by General Atomics to the NRC,[17] a licensing strategy was proposed to take advantage of the inherent safety of the HTGR and reduce the number of systems considered to perform safety-related functions. In this approach, certain functions which protect equipment but are not necessary for satisfying regulatory dose limits in accident analyses are designated as "investment protection systems" rather than "safety-related systems." Systems that are investment protection in the MHTGR include many support functions that would be safety-related systems for conventional LWRs. Specifically, the staff questioned the nonsafety classification of the block valve closure interlock system, steam generator dump and isolation valves, and system monitoring equipment for the MHTGR.

2.4.3 Concept of Operations

2.4.3.1 Integrated multiunit control

Experience with HTGRs primarily involves individual units (i.e., reactors coupled with an energy conversion/heat removal system) controlled from a dedicated MCR. The MHTGR is a notable exception. The MHTGR plant concept involves four reactor modules tied to two turbine generators. An MHTGR design goal is for a single operator and assistant to be capable of managing operational control of a multi-unit plant from the MCR. The plant I&C architecture provides for a supervisory control system to coordinate overall plant control and distribute demands among modules while individual automated control systems provide operational control for each module under normal conditions and abnormal

events. Separate, independent, redundant, fully automatic protection systems are provided for each module. Based on the safety characteristics of the prismatic core and the level of automation provided by the modular, distributed plant control system, no active manual control is required and operator responsibilities are primarily monitoring and high-level operational management.

The ALMR plant concept has a similar goal of a single operator managing a full power block. An ALMR power block consists of three reactor modules coupled to one turbine generator. The design approach for the I&C architecture of an ALMR plant is similarly based on a supervisory control system and distributed automated control of each module. Capabilities common to resilient and autonomous control, such as signal validation, command validation, control mode selection, inherent control, and fault detection and isolation, have been developed as part of past ALMR research and development efforts.

The systems requirements for the NGNP specify that manual control capabilities must be available in a single control room for an operator to take control of a reactor and its support systems. Further, the MCR must provide controls for the power conversion and heat transport systems. However, these requirements address operation of a single unit (i.e., the "reactor") and do not specify integration of control for multiple modules. The available information for the General Atomic concept of a multi-module HTGR shows a single Operations Center. There is no definitive indication of whether the concept involves separate co-located control rooms (e.g., in dedicated quadrants of the Operations Center) or an integrated multi-unit control room with common operations consoles and displays.

Current regulations address multi-unit plants. GDC 5 deals specifically with sharing of structures, systems, and components among nuclear power units. The criterion states that systems important to safety must not be shared "unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions." The potential impact of an accident in one unit affecting the safe shutdown of other units is explicitly addressed in the scope of the design criterion. Part 52 of the Commission's regulations (10 CFR 52.47) requires an analysis of "the possible operating configurations of the reactor modules with common systems, interface requirements, and system interactions." The design criteria for safety systems given in IEEE 603-1991, which are adopted as regulation by 10 CFR 50.55a(h), specifically address multi-unit stations by requiring that shared systems must not impair the capability to simultaneously perform required safety functions in all units. Other safety system design criteria that are relevant in considering shared systems in an integrated multi-unit control room include single failure, system integrity, and independence.

The positions on multidivisional control and display stations in Digital I&C ISG-04 provide key regulatory guidance that is relevant for treatment of interface support systems in an integrated multi-unit control room. Not only is it necessary to ensure independence and isolation for instances of displays (either safety and nonsafety) that can interact with multiple divisions dedicated to a single unit, but it is also necessary to address the potential impact of any interaction with safety systems associated with different units through common control and display stations. If operational control for multiple modules is integrated into a single control room with the ability to interact with I&C systems in more than one unit from a common operator console, there exists the possibility that display information and operator actions may erroneously be assigned (e.g., indicated, interpreted, commanded) to the wrong unit. In addition, failure of a common control and display station or its communication with the interconnected I&C systems could lead to spurious or failed manual commands. Clearly, the failure modes that can arise through such integrated control room systems must be identified and the consequences of those failures on plant safety must be analyzed. The guidance in ISG-04 specifies that the results of malfunctions of shared resources must be shown to "be consistent with the assumptions made in the safety analysis of the plant." At a minimum, if these types of interconnections among unit-specific systems are permitted within the main control room (MCR) of the NGNP or other HTGR plant, the regulatory guidance in ISG-04 should be extended to treat potential hazards arising from multi-unit human-machine interfaces and digital communications. In addition, the provisions of BTP 7-19, Digital I&C ISG-02, and Digital I&C

ISG-05 regarding D3 must be addressed in considering the impact of display and control stations that are common to multiple units in a plant.

In addition to its guidance on a methodology to evaluate operator action as a diverse means of coping with CCF, Digital I&C ISG-05 provides relevant guidance on evaluating the minimum inventory of human system interfaces that are necessary to support safe operation under emergency conditions and to ensure that a safe state can be achieved. Clearly, the principle of a minimum inventory of interfaces should apply at the individual unit level to ensure that timely and adequate response to plant safety challenges can be achieved. Thus, common interfaces would require detailed evaluation to confirm that the loss of a station or combination of stations would not compromise the provision of a minimum inventory of interfaces for any single unit or for multiple units.

2.4.3.2 Coupled nuclear and industrial process control

Conventional nuclear power plants are designed for the primary purpose of generating electricity through dedicated coupling of the reactor with a turbine generator via primary and secondary heat transport circuits. Most nuclear power plants are operated in base load (i.e., steady-state power production) mode, although some, particularly international, plants operate in an electrical-demand load following mode. A primary purpose of the NGNP program is to demonstrate the use of high temperature reactors for industrial process heat applications in addition to electricity production. The interconnection of nuclear plant heat transport systems to industrial process heat systems may present operational challenges due to feedback mechanisms among the coupled thermodynamic processes. In addition, the configuration of energy conversion systems to enable distinct, separate flowpaths that support multiple product streams (e.g., electricity and hydrogen production) can lead to increased complexity of the secondary circuit in a plant as well as much greater complexity of operation. For example, the heat transport system of a chemical plant for hydrogen production is very likely to be a more complex system than that required for a conventional electrical generation plant.

An integrated control room for a combined cycle nuclear plant with electrical and heat plant loads would require the automated control system to manage the load distribution and to respond to all operating events and failures of all loads. Consequently, integrated control of both the nuclear heat production systems and the end-use industrial process systems would be substantially more challenging that operating a traditional nuclear power plant in response to external electrical grid demands (i.e., a single load).

Coupled nuclear and industrial process control in an integrated control room would require treatment of the impact of the dynamic coupling in the plant safety analysis. Specifically, control and protection capabilities may be needed to mitigate the propagation of effects from operational upsets and accidents in the industrial systems and thereby minimize the potential for adverse consequences on operation of the reactor systems. For operational control, the control systems could be distinct for nuclear and industrial processes with coordination through supervisory control and/or the inclusion feedforward terms in the algorithms of distributed controllers. Protection functions could be implemented through separate, dedicated safety systems for the reactor and the industrial systems, respectively. A thorough analysis of the operational behavior of an integrated plant would be necessary to determine the necessity for any additional safety functions, in particular to address combined events. In addition, a human factors review would be needed to evaluate the appropriate roles and responsibilities for the operations staff, in particular the allocation of function associated control of both the nuclear and industrial systems.

Coupling to industrial heat processes should be considered in the plant safety analysis. In particular, the analysis should address the impact on frequency of occurrence and available response time for postulated initiating events involving loss of heat sink. The findings of this type of analysis can determine whether the capability to isolate the nuclear systems from the industrial systems should be required and whether those isolation functions should be incorporated in the plant’s safety systems.

The stated NGNP approach to incorporate industrial applications within the product stream of an HTGR plant is to treat the nuclear processes and industrial processes as separate. Specifically, the industrial process application is to be designed for implementation as an external facility separate from the nuclear facility. The intent is to adopt a paradigm in which the industrial facility is an end-use customer of heat in a manner similar to the electrical grid being an end-use customer of electricity. Thus, decoupling or isolating from the end-user/customer can serve to mitigate the consequences of external disturbances or failures.

For the NGNP, a dedicated transfer system is planned as the interposing interface between the nuclear facility and any industrial facility. Interface criteria are imposed on the transfer system to ensure that the HTGR is not adversely affected by events in the industrial facility or failure of the transfer system. If warranted by the findings of safety analysis for the nuclear facility, a capability to isolate the industrial facility must be provided. However, no portion of the transfer system that is outside the boundary of the nuclear facility is permitted to perform any safety or safe shutdown function. The NGNP approach to coupling nuclear and industrial facilities seems to minimize the complexity of design and to facilitate a more straightforward regulatory review. However, it is essential that the nuclear facility safety analysis provide coverage of postulated transients induced by failures or events arising from coupling with the industrial facility. In addition, the characteristics (e.g., severity and frequency) of those transients must be bounded by safety analysis findings.

2.4.3.3 Control room staffing and human performance

The provision of automation through modernization of existing plants and the design of extensively digital I&C architectures for new plants has engendered a transition in the roles and responsibilities of plant operators from intimate engagement in operations at the lowest control levels to plant operational oversight as a high-level supervisor who intervenes only for off-normal situations. The challenges presented by this transition to a highly automated control room are common for modernized LWRs, ALWRs, and VHTGRs. These issues include determining appropriate allocation of function between human and machine, maintaining cognitive awareness, and addressing the consequences of I&C system failure on human performance. This latter issue is of particular importance in a highly automated control room, in which the loss of control and display consoles can impact multiple indications, control access points, and information resources. Obviously, maintaining a minimum inventory of interfaces can be very challenging in modern control room design and may require development of further guidance to address new issues posed by integrated multi-unit plant management.

In the case of NGNP, the inherent safety features of the reactor design (e.g., excellent fission product retention, large margin between the operating temperature and temperature for fuel failure) may lessen the imperative for short-term intervention by the operator to mitigate accidents and other abnormal events. Nevertheless, the potential complexity involved in nontraditional concepts of operations may create new challenges to human performance. New operational scenarios that may be introduced include high-level supervision of multiple reactors, transition among different product streams (electricity, process heat) with reconfigurable balance of plant systems, and integrated plant management schemes to address phased construction and commissioning of units. Because of the potential for reduced demands on operators, which can arise from the extensive automation facilitated by digital technology and the inherent self-regulation and safety of HTGR designs, exemptions to the current regulatory staffing requirements may be requested. In particular, the potential for a single operator to manage more than one reactor may eventually be pursued. In these cases, the dependability and capability of the supporting I&C technologies must be confirmed in addition to assessment of the human factors aspects of unique concepts of operations.

2.4.4 Regulatory Framework for Highly Automated Control Rooms

The existing regulations and regulatory guidance appear to be adequate to treat the expected configuration of the NGNP control room. The NGNP program emphasizes the use of commercially available technologies and a risk-minimization design philosophy to achieve licensability. The conceptual design under development is based on heritage development from the last two decades (i.e., NPR and GT-MHR). The expectation is that the control room automation strategy will be similar to that seen for the highly integrated control rooms developed for ALWRs, which are based on digital implementations of conventional control loops and independent digital protection systems. The level of automation should be comparable to that achieved for ALWRs, with some features identified as resilient or autonomous being incorporated in the control system design to enhance efficiency and reliability. Thus, the regulatory framework applied to new plants and ALWR design certification should be sufficient for the degree of automation expected for the first-of-a-kind (FOAK) HTGR plant.

The original plan for the NGNP was to demonstrate a single unit nuclear plant coupled to a hydrogen production facility. Based on stakeholder preference, the strategy evolved to focus on commercial implementation of a multi-module plant coupled to an industrial process heat application to be selected from several options. Depending on commercial considerations, the FOAK plant may or may not involve multiple reactors. The design requirements for the NGNP indicate the use of a single control room for reactor control but there is no definitive information to suggest that integrated control of multiple units through common human system interfaces is expected. Existing regulatory guidance on intersystem communications, shared interfaces, defense-in-depth, minimum inventory, and human factors provide the basis for regulatory review of highly integrated control rooms and should be sufficient for the level of integration likely for an NGNP implementation.

The treatment of combined operation of nuclear and industrial applications could pose a challenge if the dynamic coupling between the processes is significant and the operational control is integrated. If the full range of industrial processes and systems are included within the scope of the nuclear plant, then consideration of new issues, such as chemical safety, are introduced into a nuclear plant regulatory review. Thus, the scope and complexity of a regulatory review for the NGNP would be greatly expanded over current licensing experience. However, the adopted strategy for demonstrating the use of VHTRs to support industrial process heat customers specifies that the nuclear facility and the end-use industrial facility will not be combined and operation of these facilities will be kept independent through separate control rooms. The requirements for the interconnection between nuclear systems and industrial systems for process heat applications are intended to facilitate the separation of operation through use of an interposing transfer system that can provide isolation of the nuclear facility from events in an industrial facility. Consequently, the existing regulatory framework should be suitable for treatment of nuclear plant use as a process heat supplier to an external industrial customer.

If integration of I&C systems across units and common multi-unit control and display consoles are proposed, the extension of regulatory guidance contained in the Digital I&C ISGs would need consideration to address shared I&C resources and system integration among units in addition to the current treatment of multidivisional and safety/nonsafety interconnections. As the degree of automation and integration increases, a closer coupling between human factors reviews and I&C evaluations may be warranted. Finally, if a strict separation and independence of the control and safety systems is not maintained, then additional research may be necessary to provide an adequate technical basis to evaluate the potential for functional dependencies and to assess the impact of any unique resilient design mechanisms and techniques.

2.5 KEY CONTROL AND PROTECTION MODELING ISSUES

Considerable information was gathered on I&C modeling needs for NRC licensing reviews of VHTRs or for development of new NRC guidance appropriate for the VHTR design. The approach was first to develop a set of transients that might be simulated in support of reviews of I&C system. From that list, the particular modeling features and code phenomena that are needed to represent those transients were developed. The code phenomena discussion is organized around the main components of a VHTR system. Any special code phenomenon or modeling considerations that are important for an I&C simulation, as distinct from a safety analysis model, were identified. The capabilities of two codes, RELAP and MELCOR, were evaluated in some detail. The evaluation on these two codes is based largely on their code manuals. The code manuals did not include discussions of recent additions of components for modeling gas reactors. The goal was to describe the models both in terms of their intended capability and in their mathematical formulation.

2.5.1 General Observations

For the most part, the NRC relies on applicants to demonstrate quantitative performance with a calculation or simulation when it is needed. In some instances, the NRC does perform independent studies to confirm an applicant's results. The NRC also uses its own calculation models in research for developing new regulatory guidance. The role of simulation and modeling within the NRC may increase with the review of advanced reactors because of the potential for increased complexity in the systems. For example, advanced reactor and plant system designs, including the HTGR, are expected to employ instrumentation and control systems with almost all the safety-related and nonsafety-related functions performed by digital systems—sometimes with an analog system as a diverse backup. The level of sophistication on the control side of the digital system implementations is expected to increase as the regulatory bodies have better understanding of the failure modes and mechanism of these systems.

Review of these complex systems and their potential failures will be a major challenge for engineers. In the area of control, it is expected that the plants would employ full automation of startup and shutdown transitions. The startup and shutdown modes are special control modes which the control system detects the need to switch into or out of. The complexity of these operations in conjunction ability to switch into and out of manual control smoothly makes the automation multistate event-based process. The automatic control extends over a much broader range of operations than before. Ensuring that the plant adheres to all requirements and responds safely to all challenges becomes complicated by the much more diverse range of automatic actions that a fully automated plant is programmed to perform. The roles of the I&C designer and reviewer are, likewise, increased. Ensuring that no unintended adverse interactions with safety functions and unintended violation of the plant's technical specifications becomes part of the control engineer's and the I&C reviewer's jobs.

The automation may prove to be the most challenging part of licensing the control algorithm. The need to observe and test the operation of the automation functions under a wide range of conditions will undoubtedly depend on a simulation of the operation under a great variety of normal and abnormal conditions. The NRC may find that having a plant simulation of their own is an indispensable tool in both understanding response and confirming the safety of the design in the review.

Only the I&C modeling codes were considered. The modeling overall effort is actually somewhat larger than that. I&C codes depend on other computer codes or calculations for much of the modeling input data. Parameters such as turbine performance maps, reactivity coefficients, delay neutron model parameters are produced by a sophisticated calculations in their own right. In developing an I&C modeling capability, the NRC will also have to develop the capability to calculate the parameters needed for input. Also, many input parameters have a significant uncertainty or have a normal variation over the fuel cycle or with aging. Evaluating the system interactions may require a range of values to be used to fully explore the parameter space. These parameter ranges come from other calculations and detailed

knowledge of the plant. Obtaining complete and appropriate input data for the modeling codes is always a major challenge, and this task has not been addressed in this review.

The codes that have been reviewed, MELCOR and RELAP5, have a long history with extensive qualification for modeling LWRs. The extensions and new features that have been added for modeling gas-cooled reactors have less pedigree and qualification. These versions of the code have been developed in the same nuclear safety analysis culture and have followed the same software engineering processes, but the gas reactor results should still be considered more cautiously and reviewed more carefully for accuracy and reasonableness. Additional verification studies, experience with the use of new gas reactor design features, and qualification of results against operating reactor performance when it becomes available will raise the confidence level that can be placed in the results. Also, the codes may not have all the features that are needed for all I&C studies. Additional work may be needed to develop special features for control modeling, network communications, modeling of remotely placed sensors, and other features not yet identified. At this stage of development, the available codes for I&C analysis should be considered developmental and not necessarily production codes.

Neither MELCOR nor RELAP5 is particularly well-suited for I&C analysis. Theses codes have the necessary thermal hydraulic components for the full plant simulation, but those components have a great many features that are necessary only for safety analysis in LWRs that burden the simulation and burden the user trying to develop the simulation of a plant. What is mainly needed for I&C is a simple, fast-running process model for driving a detailed model of the control system. Neither has tools for fully representing the control system in every detail nor has an interface to a control analysis tool like MATLAB/SIMULINK or sophisticated graphical user interface for representing the controls system design visually.

2.5.2 Observations on RELAP5

RELAP5 contains a set of reactor system building blocks with which to develop VHTR models that are suited for a wide range of control and protection system simulations. Models of VHTRs with near full plant scope have already been assembled and demonstrated. The single phase gas-reactor thermal hydraulics is overlaid on a structure that was developed specifically for modeling two-phase flow problem in LWRs. RELAP's hydrodynamic formulation is designed to reduce gracefully to a single phase model so that it appears that the additional capability does not hinder the gas reactor simulations. The thermal hydraulics is primarily a one-dimensional model which is entirely suitable for I&C models. RELAP5's three-dimensional version of the thermal hydraulics is limited to a coarse mesh. It is unclear if RELAP's three dimensional flow model is capable of simulating parts of VHTRs that may exhibit significant three-dimensional effects (such as the lower plenum in prismatic cores or the core region in pebble bed designs). In general, three-dimensional effects are not major concern in I&C models.

RELAP code has provided special models for gas turbines, compressors, steam generators, valves, and heat exchangers such that most configurations of the NGNP plants that have been proposed could be simulated. No chemical process models for hydrogen generation have been developed for interfacing with the RELAP code. Models of the chemical plant would be limited to boundary conditions that apply a predefined heat load to the system or a heat exchanger with predefined boundary conditions on the secondary side (i.e., predefined temperature and flow).

The range of conditions that RELAP is capable of simulating covers all the transients that are conceived of for this project. This includes all the normal and abnormal operating events and design basis accidents. For beyond design basis events such as air and water ingress, RELAP has some capability for simulating multicomponent fluids and chemical reactions so that air and water ingress events could be modeled. This capability has not been demonstrated. One of RELAPs modeling limitations that would affect the air ingress event is that a junction cannot model counter current flow for a single phase. Hence, RELAP would not be able to simulate the physics of a break in which hot gas flows out the top of the break while cold outside air flows in at the bottom of the break. Also, RELAP is generally limited to cases in which

the fuel and structures remain intact so that the full evolution of an air or water ingress would not be possible. Severe accident modeling is generally not the main emphasis of I&C cases so these limitations on modeling severe accidents are not a major concern.

Within the control simulation capability, the set of control components is fairly complete for modeling conventional controls. Components that are available in the library such as the lag and lead-lag controllers and proportional-integral controller are plug-and-play components that can be used for implementing control strategies. Like all RELAP input, the data for the controls are implemented by card image-like inputs that specify connections and parameters. However, more sophisticated control algorithms usually have more demanding computational requirements that would not be efficiently defined using these built-in control primitives. Optimal control, robust control, adaptive control, and model predictive control are just a few among these approaches. These control methods are usually avoided for controlling the primary system functions because the simpler controls are sufficient but can be implemented for the PCS, such as the turbine control. RELAP5 currently does not support the higher level control algorithms.

One of the shortcomings of the RELAP5 code system—from the control systems simulations perspective—is that it does not allow incorporation of user-created external subroutines that can perform other computations and communicate the results with the main application in a predetermined protocol. This would significantly extend the capabilities of the code system and allow design and analysis simulations of a much larger set of control systems. An interface to Matlab, for example, would allow a much greater range of control designs to be developed using the Matlab/Simulink for control development and analysis and simulation testing of the design by coupling to the RELAP5 simulation.

Another challenge in modeling these complicated systems is the communication network. In the earlier nuclear plant designs where analog control systems were used, data transfer was accomplished through point-to-point wired connections which carry a single signal. However, digital instrumentation and control systems employ fiber optic communication networks to transmit control and protection system inputs and outputs in an efficient and timely manner. The fiber optic networks carry many signals on the same network. Issues of timing, sneak circuits, and handling of missed or corrupted communications is an area of control and safety review. The review of such communications currently lacks a tool to simulate a full communication system with various rates of communications failures to show the actual consequences to the system response. RELAP does not appear to offer any tools to represent the full range of timing and delay effects of digital communications either on a network or represent communication failures.

2.5.3 Observations on MELCOR

MELCOR is a fully integrated, engineering-level computer code whose primary purpose is to model the progression of severe accidents in LWR nuclear power plants. It is specifically designed to represent accidents that proceed to core degradation and relocation of structural components. Recent additions to the code have made it possible to simulate gas-cooled reactors. These additions include additional material properties for helium coolant and the reaction products needed for severe accident analysis and special component models for a full plant simulation. The new component models include axial flow turbomachines, a counter-flow heat exchanger, neutron point kinetics, pebble fuel heat transfer, and two chemical processes for hydrogen production. Even though the modeling structure contains the special features for degradation and relocation fuel and structure that are largely unneeded for I&C models, the code is also capable of modeling the normal and abnormal operating events and design basis events that have been proposed in this report as needed for the I&C modeling tool for the NRC. The one-dimensional hydrodynamic equations and the numerical solution technique are suitable for I&C calculations over a wide range of conditions.

The control simulation capability for MELCOR is fairly limited. It includes standard blocks for the basic arithmetic operations and special control operations such as hysteresis, PID control, and trips. In contrast to RELAP5, however, MELCOR has the capability for user-defined functions. These functions are used

both to simulate the actual controls system and to simulate physical processes that are not contained in the supplied process models. The control functions, for example, are used for the pebble fuel heat transfer model. The control functions are limited to a maximum of five real inputs, which would seem to limit their usefulness in general programming. Just as in RELAP, MELCOR would also benefit from an interface to a more user-friendly control modeling environment such as MATLAB/SIMULINK.

The turbine and compressor models are somewhat unique compared to usual practice in I&C modeling codes. The model is basically a turbine design tool that has been incorporated as a time dependent model. The model may require a more sophisticated understanding by the user of turbine design and calculations than a more traditional performance map model. Also the code is based on quasi-steady rather than dynamic conservation equations. The quasi-steady approach to modeling the fluid would not be satisfactory for fast turbine control events such as turbine trip or loss of secondary flow. The model is suitable for slow power maneuvering transients, steady state thermal cycle analysis, and events in which the turbine dynamics are of secondary importance. The capability for modeling steady state, off-design conditions is better in MELCOR than in the typical performance map model because of the built-in turbine design correlations.

The chemical process models for hydrogen production and their description is a useful addition to the modeling library, particularly the explanation of the reaction rate equations and the data for chemical models. However, the models do not seem fully integrated with the concept of a transient code for full system modeling. One of the approximations in the chemical model is constant pressure in the reaction chamber. This assumption would prevent simulating the actual pressure controls that might be the subject of an I&C model of the hydrogen process or simulating any event that initiates a pressure disturbance in the chemical reaction chamber.

3. SUMMARY AND CONCLUSIONS

This project supported the NRC in identifying and evaluating the regulatory implications concerning the control and protection systems proposed for use in the NGNP. Specifically, the report provided insights into the control and protection systems likely to be used in the NGNP, including information on systems to be used in the reactor and process heat applications as well as guidelines for the design of highly integrated control rooms. The work is to aid the NRC in developing new regulatory guidance in reviewing NGNP license application. This NRC project also evaluated reactor and process heat application plant simulation models, but details of this work were not included.

Although similarities exist, many aspects of modular HTGR heat transport system controls are quite different from those of LWRs. These were noted, and I&C details of the 1980s DOE design of the MHTGR provided for interconnected and integrated automatic control of four reactor modules and two turbogenerator systems comprising the plant.

While the most likely NGNP initial design has a steam generator in the primary loop, similar in many ways to the MHTGR, controls for the other major type of power conversion proposed for modular HTGRs, the direct-cycle gas turbine, were also described.

4. REFERENCES

1. *Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors*, IAEA-TECDOC-1366, Vienna, Austria, August 2003.
2. D. E. Holcomb, M. S. Cetiner, and S. J. Ball, *HTGR Measurements and Instrumentation Systems*, ORNL/TM-2012/107, Oak Ridge National Laboratory, March 2012.
3. *Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology*, IAEA-TECDOC-1198, Vienna, Austria, February 2001.
4. E. Ziermann, "Review of 21 Years of Power Operation of the AVR Experimental Power Station in Julich," *Nuclear Engineering and Design*, **121(**2), 135–142 (July 2, 1990).
5. *MHGTR Conceptual Design Package: Plant Control, Plant Protection, & Plant Monitoring Systems*, issued by Gas-Cooled Reactor Associates for the Department of Energy, Contract DE-AC03-78F02034, December 1987.
6. *Accident Analysis for Nuclear Power Plants with Modular HTGRs*, International Atomic Energy Agency, IAEA Safety Report Series No. 54, Vienna, Austria, 2008.
7. S. M. Mitchell and M. S. Mannan, "Designing Resilient Engineered Systems," *Chemical Engineering Progress*, **102(**4), 39–45 (April 2006).
8. C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient Control Systems: Next Generation Design Research," pp. 632–636 in *Proceedings 2nd Conference on Human System Interactions*, Catania, Italy, May 2009.
9. J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien, *Roadmap to Secure Control Systems in the Energy Sector*, prepared for the Department of Energy by Energetics, Columbia, MD, January 2006.
10. C. G. Rieger, "Notional Examples and Benchmark Aspects of a Resilient Control System," pp. 64–71 in *Proceedings of 3rd International Symposium on Resilient Control Systems*, Idaho National Laboratory, Idaho Falls, ID, August 2010.
11. "Preliminary Safety Information Document for the Standard MHTGR," Chapter 7 in *Plant Protection, Instrumentation, and Control*, DOE-HTGR-86-024, Stone and Webster Engineering Corporation, 1986.
12. *Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, Office of Nuclear Reactor Regulation, Washington, DC, December 1995.
13. *Conceptual Design Summary Report, Modular HTGR Plant, Reference Modular High-temperature Gas-cooled Reactor Plant*, DOE-HTGR-87-092, Bechtel National, Inc., under subcontract to Gas-Cooled Reactor Associates for the Department of Energy, Contract DE-AC03-78SF02034, September 1987.
14. *Probabilistic Risk Assessment of the Modular HTGR Plant*, DOE HTGR-86-011 Rev 1, issued by GA Technologies, Inc., for the Department of Energy, Contract DE-AC03-84SF11963, June 1986.
15. *Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, December 1995.
16. J. Stang, U.S. Nuclear Regulatory Commission, letter to Dave Baxter, Duke Energy Carolinas, "Oconee Nuclear Station, Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the

Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade (TAC Nos. MD7999, MD8000, AND MD8001)," January 28, 2010.

17. *Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, December 1995.