INL/EXT-05-00764

Instrumentation, Control, and Intelligent Systems

Harold S. Blackman

September 2005

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

INL/EXT-05-00764

Instrumentation, Control, and Intelligent Systems

Harold S. Blackman

September 2005

Idaho National Laboratory
Idaho Falls, Idaho 83415

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

INL's Mission and Instrumentation, Control, and Intelligent Systems

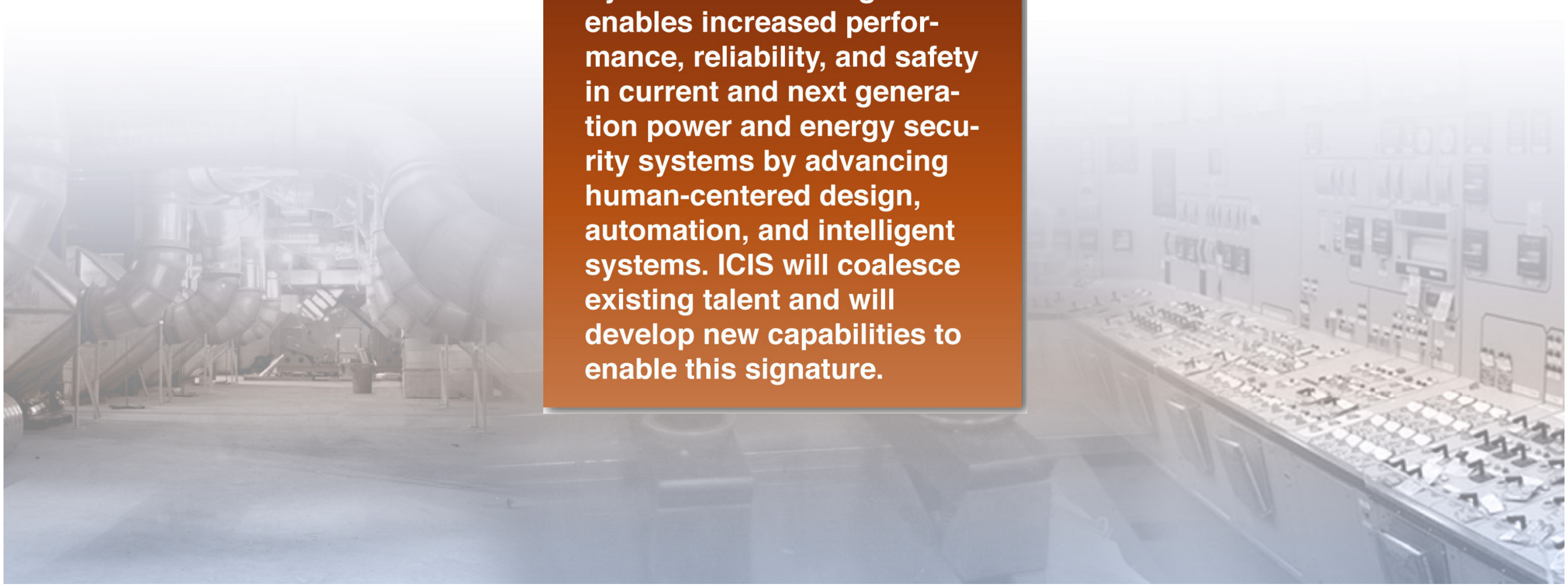
Abundant and affordable energy is required for U.S. economic stability and national security. Advanced nuclear power plants offer the best near-term potential to generate abundant, affordable, and sustainable electricity and hydrogen without appreciable generation of greenhouse gases. To that end, Idaho National Laboratory (INL) has been charged with leading the revitalization of nuclear power in the U.S.

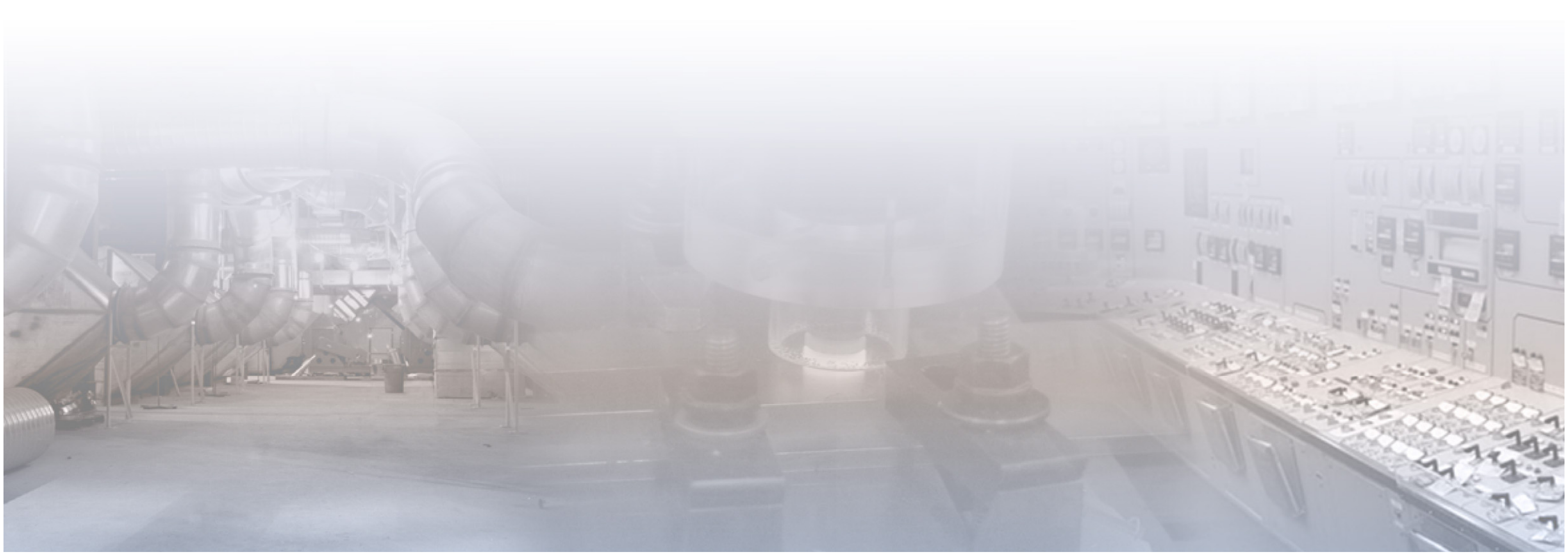
The INL vision is to become the preeminent nuclear energy laboratory with synergistic, world-class, multi-program capabilities and partnerships by 2015. The vision focuses on four essential destinations:

- Be the preeminent internationally-recognized nuclear energy research, development, and demonstration laboratory
- Be a major center for national security technology development and demonstration
- Be a multi-program national laboratory with world-class capabilities
- Foster academic, industry, government, and international collaborations to produce the needed investment, programs, and expertise.

Crucial to that effort is the inclusion of research in advanced instrumentation, control, and intelligent systems (ICIS) for use in current and advanced power and energy security systems to enable increased performance, reliability, security, and safety. For nuclear energy plants, ICIS will extend the lifetime of power plant systems, increase performance and power output, and ensure reliable operation within the system's safety margin; for national security applications, ICIS will enable increased protection of our nation's critical infrastructure. In general, ICIS will cost-effectively increase performance for all energy security systems.

Idaho National Laboratory has been charged by the Department of Energy with leading the revitalization of nuclear power in the United States. The Instrumentation, Control, and Intelligent Systems Science Signature enables increased performance, reliability, and safety in current and next generation power and energy security systems by advancing human-centered design, automation, and intelligent systems. ICIS will coalesce existing talent and will develop new capabilities to enable this signature.





CONTENTS

FIGURES

TABLES

ACRONYMS

ATR	Advanced Test Reactor
DOE	Department of Energy
HMI	human-machine interface
I&C	instrumentation and controls
ICIS	Instrumentation, Control, and Intelligent Systems
INL	Idaho National Laboratory
NRC	Nuclear Regulatory Commission
R&D	research and development
SCADA	supervisory control and data acquisition systems
UAV	unmanned aerial vehicle
UGV	unmanned ground vehicles
VHTR	very high-temperature reactor

Instrumentation, Control, and Intelligent Systems

VISION

The Instrumentation, Control, and Intelligent Systems (ICIS) science signature will lead the development of advanced instrumentation, control, and intelligent systems to support next-generation power and energy security systems. Idaho National Laboratory (INL) will advance current instrumentation and control methods that focus on controlling sub-processes and components by designing and implementing intelligent systems in which the state of the entire process is optimized. This vision will be accomplished by increasing performance, reliability, security, and safety through critical human-centered design, automation, and intelligent systems investments, as shown in Figure 1.

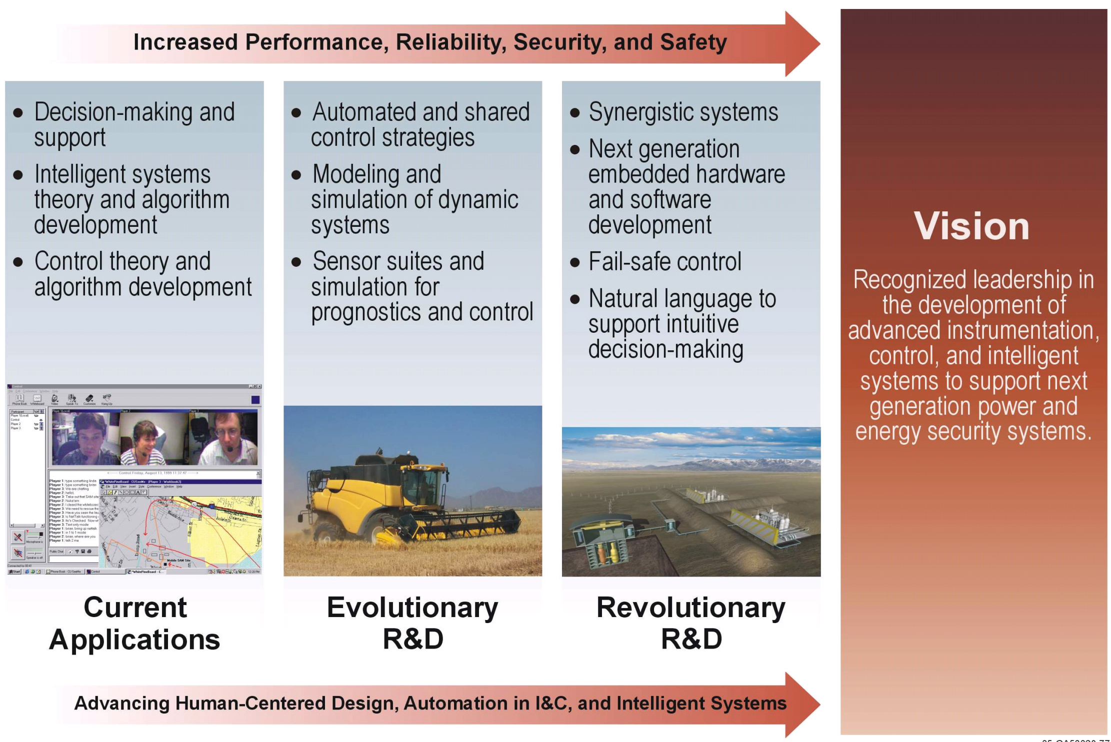


Figure 1. The ICIS science signature increases performance, reliability, security, and safety of power generation and energy security systems.

Provide Systems Solutions for Nuclear Energy, National Security and Energy Security Programs

Cost-effective and inexpensive increases in system performance, reliability, security, and safety result from ICIS research and development (R&D). Relatively small investments in hardware and software leverage the billions of dollars invested in nuclear, national security, and energy security systems. In many of these systems, any accident or failure is unacceptable; thus, ICIS investments are required. Table 1 summarizes needs for current, evolutionary, and revolutionary ICIS R&D in our Department of Energy (DOE) mission focus areas. ICIS research activities, though initially focused on unique nuclear energy, national security, and energy security needs, will have broad application across all three areas.

Table 1. Nuclear energy, national security, and energy security challenges and solutions provided by ICIS.

INL Mission Focus	ICIS R&D Stages	Critical R&D Accomplishments for Each Stage
Nuclear Energy	Current Applications	Update current control systems to provide operators with predictive systems so they can reliably determine the health of processes during both gradual and abrupt changes
	Evolutionary	Provide system quality measurements as inputs to a lifetime prediction model that then optimizes process parameters to extend the lifetime of the nuclear plant
	Revolutionary	Enable reliance on digital systems and automation required to support a “100-person” plant for the very high-temperature reactor concept
		Develop systems that anticipate and mitigate the effects of potential system failures to optimize plant efficiency, maintain high availability, and ensure system safety margin
National Security	Current Applications	Test full-scale physical security and cyber infrastructure systems, determine weaknesses, and develop methods to protect systems from malicious and unintentional attacks based on quantifiable prioritization of safety and economic concerns
	Evolutionary	Develop efficient and secure nuclear fuel cycle monitoring systems with integrated safeguards and proliferation detection solutions that provide real-time material accountancy techniques to increase safety
		Develop supervisory control and data acquisition system (SCADA) control technologies that support the paradigm shift from “resist to attack” to “survive and adapt” in secure control system designs to maintain reliable process performance
	Revolutionary	Proactively recognize and respond to a potential threat before a control system is compromised, ensuring system integrity
Energy Security	Current Applications	Develop sensors capable of surviving for long periods in severe environments (i.e., extreme temperature, radiation, harsh chemicals) and capable of monitoring more than one process parameter
	Evolutionary	Research and design sensors, control systems, and algorithms that allow plants and autonomous systems to operate at the plant design point by reducing measurement uncertainty
		Implement condition-based maintenance strategies to increase performance and reliability
	Revolutionary	Reduce operator burden and increase operator situational awareness by developing interfaces that incorporate high level, plain language commands, voice recognition capabilities, and bi-directional human/control system communications
		Develop sensors and controls with the ability to recognize and adapt to the health of systems, resulting in significant increases in system efficiency, lifetime, reliability, security, and safety.

Enable Energy Security and Economic Growth

Because of the potential to realize tremendous cost benefits, process efficiency, productivity, and safety gains, ICIS is a critical enabler of control systems required for future energy production and security. For example, next-generation nuclear power plants must be stable, secure, and fail-safe to gain public support. This requires ICIS designs that use redundant and diverse technologies that consider the security and safety impact of a failure and sensors and controls that are able to predict failure and continue to perform, even in unforeseeable accident conditions. The information collected by these systems must then be presented to the operators in a way that will support accurate and timely decision-making.

Industrial applications of intelligent systems are also of great importance to the economic success and competitiveness of the U.S. Our nation must be first to develop new ways to increase the performance, reliability, security, and safety of manufacturing and processing systems, resulting in increased productivity, reduced energy consumption, and reduced overall cost.

Improve Performance, Reliability, Security, and Safety

ICIS offers the opportunity to make revolutionary changes in current operating methods for many complex systems; it offers the opportunity to move from current component control approaches to an overall system control approach, and changes how humans interact with dull, dirty, or dangerous processes. The reliability, productivity, security, and safety of such systems will be improved enormously by introducing intelligent controls and instrumentation that provide humans with just the right information at just the right time to make the decisions necessary to support a process. This roadmap lays out the required strategies, research areas, and capabilities necessary to achieve these advances.

PATH TO SYNERGISTIC SYSTEMS

Four processing components are essential to control—sensing, perceiving, deciding, and responding. Connecting each component are communications pathways or interfaces. Current control strategies depend on the human, in large part, to perceive and decide, and depend on system components to sense and respond. The control strategies have resulted in intelligent machines or systems that either know, or can learn, to perform a mission or task. For example, an autonomous system is one that can operate in a mechanistic and unintuitive manner without human intervention based on being preprogrammed or incorporating basic learning capabilities. But the absence of the human involvement limits the dynamic nature of responses from an autonomous system.

Albus (1991) defines intelligence as "the ability of a system to act appropriately in an uncertain environment, where appropriate action is that which increases the probability of success, and success is the achievement of behavioral sub-goals that support the system's ultimate goal."

The ICIS nexus strategy, i.e., interconnecting sensing, perceiving, deciding, and responding, enables a new class of process intelligence—synergistic systems. These synergistic systems are a revolutionary class of intelligent systems or machines involving human intervention, where, through cooperative actions, the total effect is greater than the sum of two or more actions taken independently. Thus, a synergistic relationship between a human and an intelligent machine enables an operator to perform a task or mission more reliably, efficiently, securely, and safely than would be the case for either a human, alone, or an autonomous machine, alone.

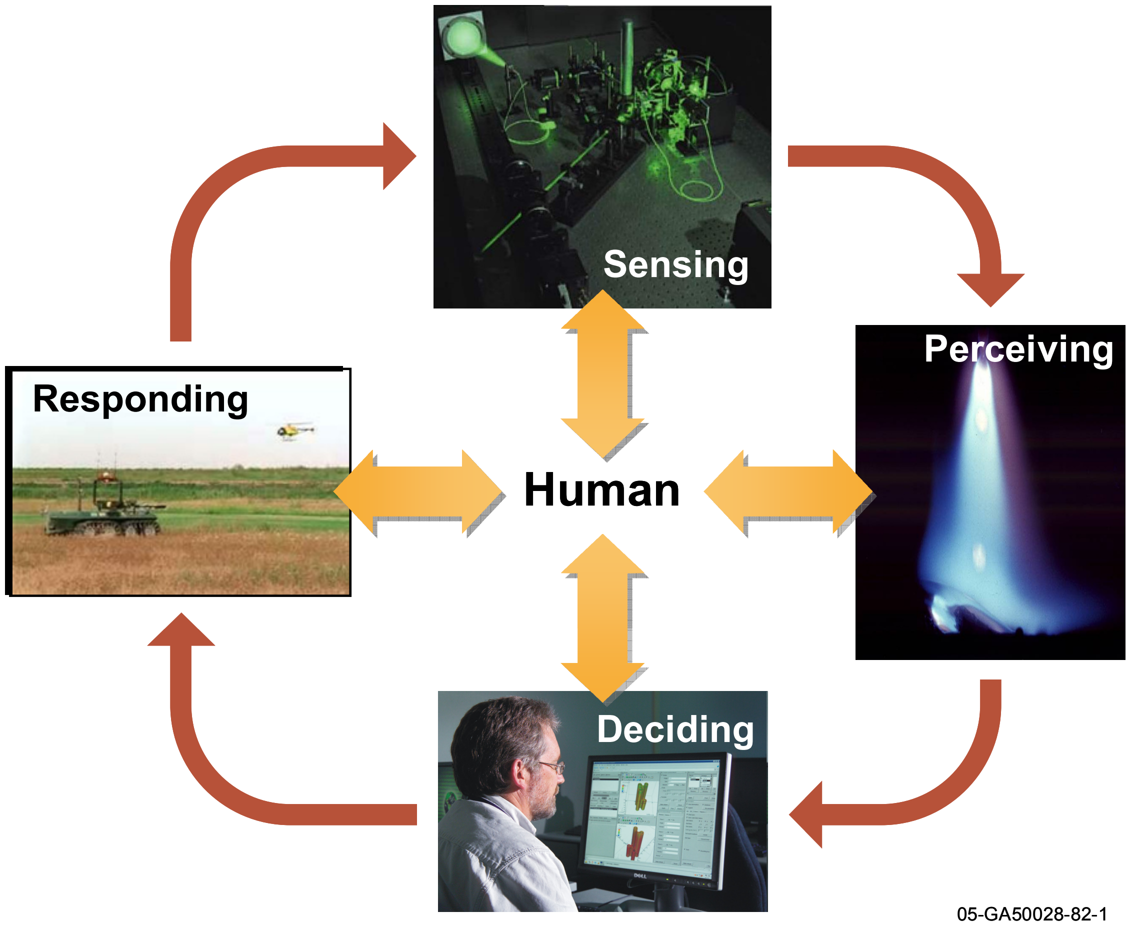


Figure 2. The ICIS nexus unites sensing, perceiving, deciding, and responding in a synergistic human-centric system through interconnecting interfaces.

Optimize System Performance, Reliability, Security, and Safety Using the ICIS Nexus Strategy

ICIS nexus strategy, as shown in Figure 2, enables revolutionary, human-centric approaches to system operation and performance. Sensors provide data to the system through an interface, and the data may be displayed via instrumentation and then acted upon by a controller, either automatically or manually. This process is analogous to the way in which humans behave. We, as humans, receive input from our senses. This information is then processed through our nervous system, including sensor processing and cognitive processing, leading to a decision that is executed through an interface of some sort, which then results in another opportunity to sense change in the system. ICIS will focus on the nexus elements—sensing, perceiving, deciding, and responding—and will improve system designs by making them human-centered ton reflect the way in which humans expect information to be processed.

To that end, ICIS research will develop synergistic systems for nuclear energy, industrial, energy security, national security, and defense applications that move us from the current mechanistic and unintuitive controls to new classes of robust, fail-safe systems that can be easily operated by humans in synergistic and productive ways, as shown in Figure 3.

Today	2015
• Mechanistic and unintuitive controls • Controllers that fail • Sensors that must be validated and calibrated • Robotic systems dependent on the human	• Natural human interfaces to allow efficient interaction • New class of robust, fail-safe, secure controllers • Advanced self-calibrating and self-validating sensors • Synergistic and autonomous systems for unstructured environments • On-line condition and process monitoring

Figure 3. By 2015, ICIS develops synergistic systems that are integral to nuclear energy, industrial, energy security, national security, and defense applications.

Essential Elements of the ICIS Nexus Approach

Realizing a new class of synergistic systems requires enabling research in these nexus elements: sensing, perceiving, deciding, and responding.

Sensing

Sensing requires new, better, and more capable sensors, as shown in Figure 4. Revolutionary sensor strategies must bridge the gap between traditional disciplines like physics and biochemistry to reveal novel processes and relationships among systems. Great value will be gained by understanding and improving upon the sensor devices, feedback systems, and logic used by biological organisms.

For industry, sensors must be capable of surviving for long periods in severe environments (i.e., extreme temperature, radiation, harsh chemicals).

For scientific research, new sensors will be needed that are capable of resolving details of the structure and composition of materials at the micro, nano, and molecular level and for guiding the fabrication of advanced materials.

Thus, next-generation sensors must have the ability to:

- Perceive, process, and decide
- Fuse multiple sensing phenomena and the required sensed parameters into a unified measurement
- Move beyond simple sensing of a single phenomenon

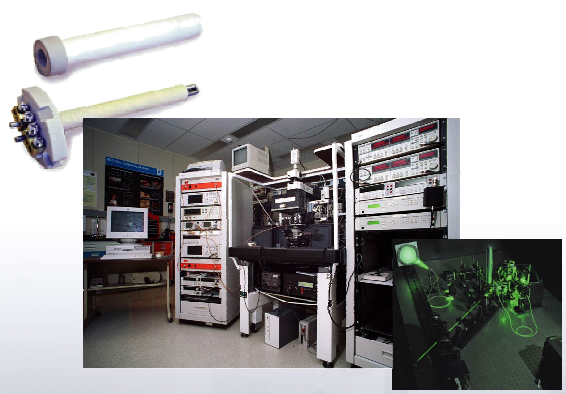


Figure 4. INL uses a range of sensors, from simple, commercial, ceramic sheathed thermocouples to complex research systems like the INL Imaging Ultrasonic Microscope or the INL Laser Ultrasonic Camera to sense process parameters.

- Provide accurate information over long use periods in harsh environments, where sensor drift and sensor corruption may dominate sensed values
- Track and predict sensor corruption (e.g., provide self-validation and self-diagnosis data)
- Estimate their own confidence level for the accuracy and validity of each measurement made
- Sense process dynamics and report those dynamics back to the ICIS process flow
- Incorporate advanced signal analysis and filtering techniques
- Be more robust
- Possess novel power and communication methods
- Be networked and collaborative
- Provide improved assurance of signal validity
- Be capable of detecting out-of-bounds conditions and warning of this state.

Revolutionary Sensors Do More than Sense

Next-generation sensor systems will encompass not only sensing, but perceiving, processing, and deciding elements, as well. Sensing systems need to move beyond simple sensing of a single phenomenon. These systems will have the ability to fuse multiple sensing phenomena and the required sensed parameters into a unified measurement. Additionally, there is a need for sensors that provide accurate information over long use periods in harsh environments where sensor drift and sensor corruption may dominate sensed values.

Next generation sensors will actually sense process dynamics and report those dynamics back to the ICIS process flow. This is a large step, beyond simply sensing a single phenomenon, such as temperature, or fitting sensed data to predetermined models.

Future sensor systems will provide the ability to sense whole process states and system dynamics.

Next-generation sensor systems will use new, more generalized mathematical embedding techniques to determine a process's fundamental relationships. By using these relationships, automatic formulation of differential equations that predict those relationships should be achievable. Such advanced sensor systems will become key enablers for self-calibrating, self-healing, plant-drift correction, and restabilization of ICIS systems during normal and unexpected plant operations.

Perceiving

Perceiving—the act of becoming conscious of or recognizing or discerning—and perception—the act of intelligent or intuitive discernment—imply a capability beyond mere observation. Traditional sensing may involve processing data to assist a human in recognizing or characterizing it. Prior knowledge of specific objects or a class of objects is inherent in essentially all current object recognition methods. Recognition may be based on the assumption that an object having certain characteristic features must be of a certain type. In such an approach, a catalog of all objects expected in an environment is used, together with algorithms that look for certain characteristic features. If an object does not have such features, it will not even be recognized as an object, much less be identified.

Future control systems will incorporate a new generation of sensors that not only perceive objects in their operating environments, but also discern the state of plants and processes. For example, the molten metal droplets shown in Figure 5 are typical of spray transfer, suitable for welding of thick section structural steel. Perception is well beyond the capabilities of traditional sensors, which simply provide data.

INL has been conducting research for several years on the development of advanced mathematical methods for recognition of objects in a plant's operating environment and automatic defect recognition and classification in nondestructive examination systems for inspection of welds and steel tubing.

Figure 5. Optical sensing used to perceive the detachment of liquid metal droplets during spray transfer in gas metal arc welding.

Perception in Next-Generation Sensors

The major functional capability that needs to be developed to enable perception is a method for recognition and classification of novel objects. These novel objects may be:

- Physical objects in the plant's operating environment
- Flaws or defects in a material undergoing a process
- Features in a sensor signal.

In future sensor perception strategies, data will be automatically processed to identify objects, states, and events. In addition, the sensors will provide their control systems with confidence levels associated with their identification and classification outputs, verification that they are properly calibrated, and characterization of their health.

Fundamental research in cognitive processes and significant breakthroughs in algorithm development will be needed to solve this problem to support revolutionary new control methods.

Deciding

To maximize system availability, performance, and productivity, it is critical to maintain adequate situational awareness to make effective decisions. In a nuclear energy application, situational awareness may imply recognizing the health status of plant components. In a threat circumstance, situational awareness may mean identifying the location, capability, and condition of enemy forces.

Implementing situational awareness methodologies in modern dynamic systems poses new challenges, as the target applications are complex and consist of collections of distributed components that can operate in multiple regimes.

Advances in current online condition monitoring require research in the following areas to develop synergistic decision schemes:

- Pattern recognition – to decouple and recognize process and control anomalies and sensor drift using observed and predicted information, resulting in decisions that keep processes within acceptable limits
- Learning machines – to expand noise analysis and verify online the calibration of instruments over their entire operating ranges, resulting in significant reductions in the costs associated with hands-on instrument calibrations and improvement in plant safety by promptly revealing calibration drifts

- Anomaly detection, diagnostics, and prognostic methods – to implement process and security integrity monitoring that provides online condition monitoring and detection of operations anomalies to discern process malfunctions or facility misuse, using both time-driven and event-driven dynamics.

Current technologies to decide the health of systems are either data-driven or model-driven. Under data-driven schemes, a representative model of the observed process is derived from the recorded data, itself, with little attempt to understand the physical relationships governing the underlying system. Common technologies used to implement data-driven solutions are neural networks and regression methods. Under model-driven schemes, a model of the monitored process is derived from governing (physical or logical) equations regulating the process.

INL has strong development expertise in the area of advanced technologies for online condition monitoring. For example, the adaptive and enhanced performance characteristics of hybrid schemes (combined data-driven and model-driven schemes) have been demonstrated in actual settings, as shown in Figure 6. Technologies for predictive maintenance have also been investigated and their numerous benefits demonstrated.

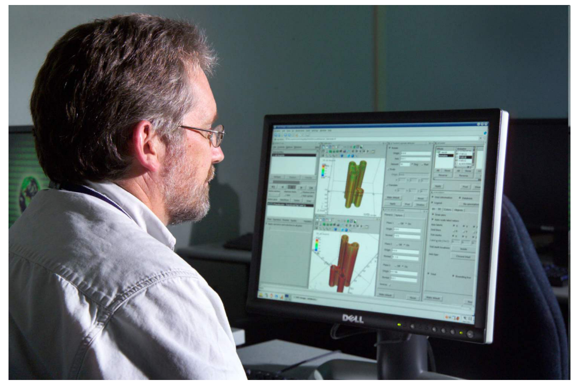


Figure 6. ICIS condition monitoring provides operators with visualization tools to aid in the decision process.

Dependability is Critical to the Decision Element

To avoid frequent or severe failures and long outages, systems must be dependable. Next-generation online condition monitoring must track operational parameters; signal static or evolving anomalies; predict system component future conditions, including deteriorations and malfunctions; and identify the nature of the anomaly and probable causes and consequences, if not addressed, to ensure system dependability.

Responding

In traditional control systems, perceiving and deciding elements occur off-line using predetermined actions, thus, limiting responses to off-normal events. These designs relegate complex plant control to preplanned offline process flows that focus on sub-process understanding and stabilization approaches, rather than on overall process optimization. This approach greatly limits the efficiency, agility, and optimality of the processes being controlled.

Figure 7. Intelligent machines, such as unmanned ground and aerial vehicles, provide response capabilities to keep humans from harm.

Responding actions may be initiated via feedback or closed-loop mechanisms to influence system behavior. Three broad classes of response include:

- Control - actuators located throughout a plant are manipulated in order to regulate process variables and meet performance requirements
- Maintenance - estimated and predicted process health information is used to schedule maintenance activities in an optimal manner

- Information operations - offensive responses are delivered to collect intelligence about the adversary and to weaken or incapacitate its capabilities, as shown in Figure 7.

INL has strong expertise in the development and demonstration of advanced control, maintenance, and information operations strategies. For example, in the area of information operations, INL is assessing and developing guidelines, methodologies, and tools as part of the critical infrastructure protection program, including wireless and control system components, to discover vulnerabilities and suggest remedies. Based on this large body of knowledge, tools to counter computer network exploitation and computer network attack can be produced.

Next-Generation Responding Strategy

Many of the processes that will need advanced controls are highly unstructured, distributed, and inherently nonlinear, with massive numbers of internal states. To move from the current approach to next-generation responding strategies, these systems must have the ability to self-heal and respond to off-normal events in a self-stabilizing fashion.

Scientific and technological advances required to perform actuation in a completely secure and stabilized fashion are:

- Controller use of both sensed process parameters and sensor confidence levels
- New, distributed stability theories
- New, self-discovering, nonlinear control theories that can interact with automated dynamics-finding sensor systems
- New, symbol-based approaches to system dynamics and their related control theories
- More secure distributed communication protocols and networks
- New, redundant control system architectures that consider the safety and security impacts to operability
- Small footprint, high performance computational packages and languages to replace outdated programmable logic controllers
- New computational and programming methods to estimate and mitigate calculation uncertainty within controller and plant models
- Next-generation actuation units (e.g., shape memory actuators and polymer-based artificial muscles)
- New industry standards for risk-based instability acceptance criteria
- New industry standards for plug and play instrumentation and controls (I&C) implementation hardware.

Interfaces and Processing

Integration of sensing, perceiving, deciding, and responding in a human-centric, synergistic system requires seamless interfaces to processes. Interfaces define the pathways by which two or more unrelated entities interact or exchange information. They may be unidirectional or bidirectional, and exchanges of information may be occurring concurrently between multiple entities. Decisions are made based on the information exchanged, so achieving the desired result depends on the quality and timeliness of information received. At each end of an interface is an interpreter, where the exchange of information is regulated and placed in a format for processing.

Traditional control systems are made up of several synchronous interfaces to regulate the flow of information and ensure its delivery and integrity. These interfaces can generally be described as the field device or sensor interface, input/output interface, controller interface, and data highway or human machine interface (HMI), as shown in Figure 8. Often these interfaces are proprietary.

Processing is the ability to manipulate data and execute instructions, forming the basis for the intelligent interactions that exist to accomplish sensing, perceiving, deciding, and responding. Processing activities occur on control system devices such as the HMI or controller. The HMI is the user interface, using graphics for the display of sensor data and input of user responses. The controller is the process interface, perceiving data from multiple sensors for display by the HMI, and issuing responses based on user input and logic constraints that define the safe operating envelope for the control system.

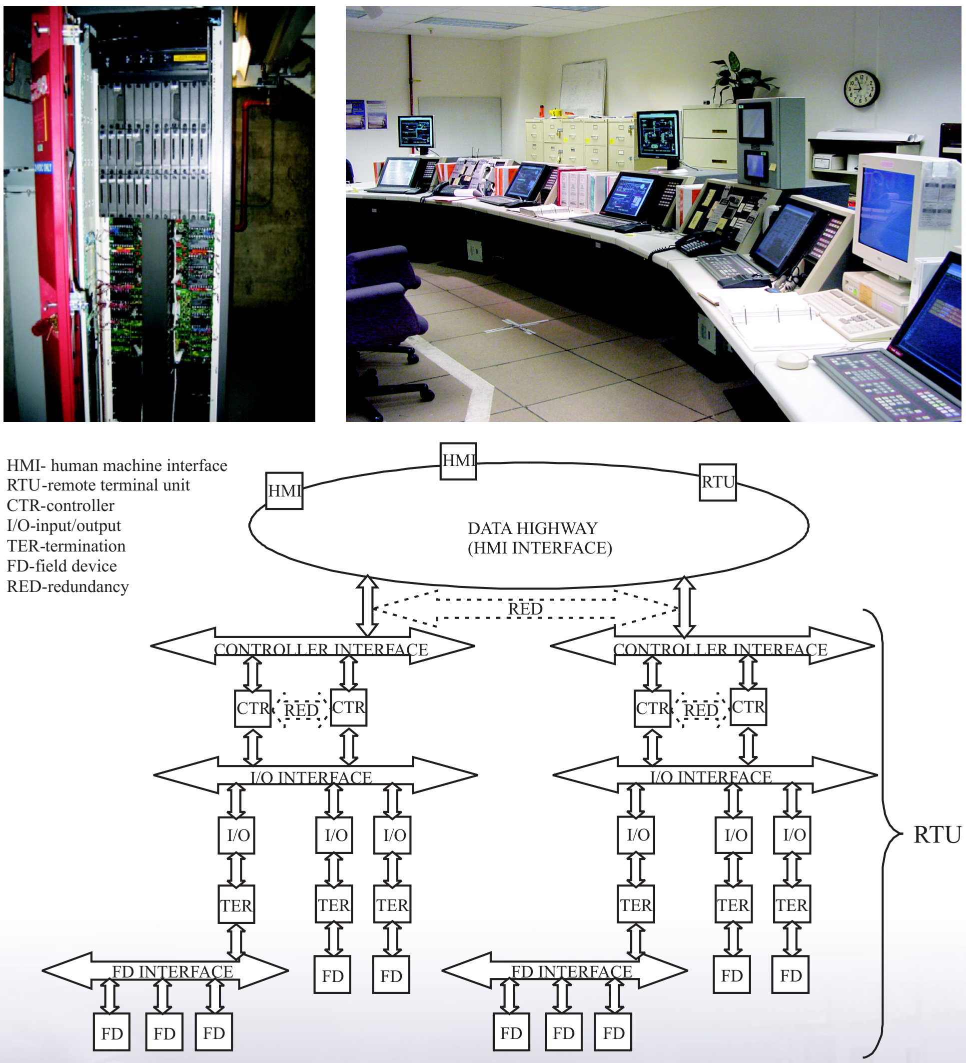


Figure 8. Interfaces and system architecture are critical to system control.

Next Generation Control Systems

In recent years, the desire for interoperability, choice, and cost reduction has led to several changes in the system architecture of traditional control systems. The HMI, which was often based on proprietary hardware, is now typically based on personal computer hardware.

Distributing the processing capacity to lower levels of the system architecture requires fewer remote terminal unit controllers, reserves the processing power for higher order functions, such as advanced control algorithms, and distributes the rudimentary control functions to the sensor interface. Where redundancy was once prescribed at the controller level, it can now be prescribed at the sensor level, thus, reducing cost. At the same time, processing capacity continues to increase with technological advances, allowing more instructions to be executed in less time. Sensor interfaces are using open system protocols, allowing the selection of a variety of vendors, depending on their product's cost and features.

The future of interfaces and processing will see continued distribution of processing capacity and advanced control implementation at the field-device level. Achieving an advanced distributed approach requires:

- Smart field devices to assume remote terminal unit control functions and interface directly with the HMI
- Global stability and supervisory control performed at the HMI level
- Development of faster and more flexible field device interfaces
- Research to achieve advances in parallel processing techniques
- Smart field devices that incorporate the ability to monitor and respond intelligently to changes in the quality of information it processes, incorporate self-healing techniques, and implement security measures that accept an interface only with an authorized HMI and reject rogue sources.

Intelligent Machine Applications

Intelligent machines can adapt to changing conditions, ascertain a plan, make decisions on a best method, and carry out the plan through physical actions. They extend the concepts of perceiving and deciding to a semi-autonomous or autonomous form, allowing them to interact with their environment with limited initial guidance. Through the use of soft computing techniques, they extend the mathematical basis of hard computing to include a human-like developmental mechanism for gaining an understanding of their environment within a defined universe.

Future research in fusion of soft and hard computing techniques will be required to improve a machine's ability to perceive and decide. The defined universe of an intelligent machine is limited by the task and the technology available for perceiving the environment and deciding on a physical action. Ideally, with the fusion of techniques, the only limitation would be the task the machine is to perform (e.g., a machine designed for welding would not be used for turning bolts).

Research in varied methods of sensing individual environmental variables will aid in this interpretation and adaptation, in an effort to reproduce subtle aspects of the environment that may otherwise not be recognized. In a simple form, for an unmanned aerial vehicle (UAV) that operates both near the ground and at high altitudes, two techniques would be used for measuring the altitude so that the best overall accuracy is achieved in both operating conditions.

Processing capacity for an intelligent machine will be distributed to allow advanced control algorithms and modeling to improve performance at the field-device level, thus, quickly perceiving changes in environmental variables and promptly deciding on an action.

Value of Synergistic Systems

Fully synergistic systems provide the opportunity to produce fail-safe controls. Traditional control systems may fail because of changes in the dynamics of the plant being controlled, component failure, or misdirection, either accidentally or on purpose, by the human operator. Synergistic systems, based on the ICIS nexus strategy, will provide fail-safe, secure operation by addressing internal and external failure mechanisms and incorporating high-level optimization capabilities to increase energy efficiency and productivity.

Figure 9 presents ICIS nexus elements incorporated into an industrial steel-making process in which some intelligence has been added to the perceiving and deciding elements. This system moves beyond a traditional control system in which control laws and actuators focus on sensing and responding. In this industrial control application, INL includes integration of the human-in-the-loop, taking the first steps in developing a true, albeit primitive, synergistic system. It is our long-term objective for machines to become very good at both "perceiving" and "deciding," in addition to their present strengths of "sensing" and "responding."

The four nexus elements and their interfaces and processes enable intelligent control systems and machines that work synergistically to realize increases in performance, reliability, security, and safety.

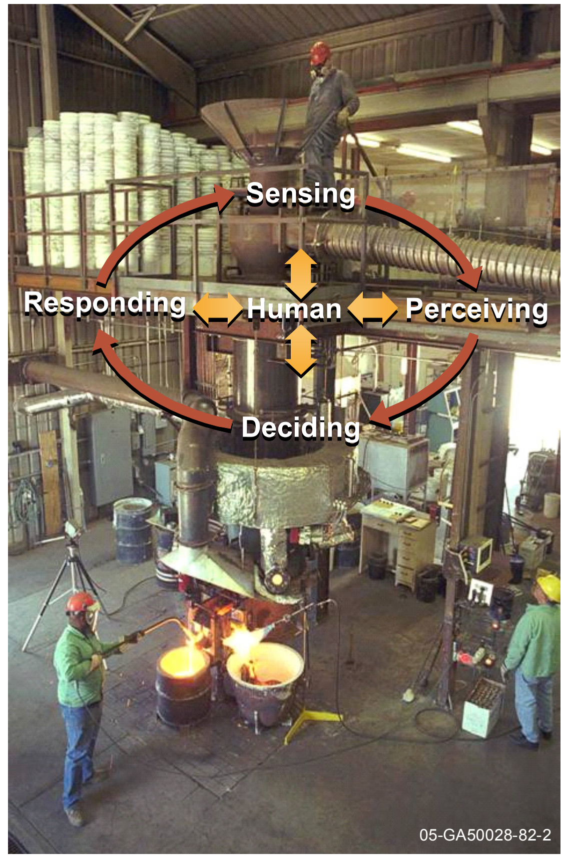


Figure 9. INL has worked with industry to incorporate ICIS nexus elements into the control of steel-making in a cupola.

ICIS RESEARCH AND DEVELOPMENT AREAS

To realize this new class of synergistic, intelligent systems, ICIS focuses on five R&D areas aligned with INL's nuclear energy, national and homeland security, and energy security goals:

- Nuclear Energy and Nonproliferation Systems
- Industrial Process Monitoring and Control
- Threat Detection and Mitigation
- Autonomous and Semi-Autonomous Robotics and Intelligent Machines
- Human-Centric Interfaces and Controls.

Nuclear Energy and Nonproliferation Systems

ICIS nuclear energy and nonproliferation systems research is a critical element in deploying future nuclear systems and increasing the reliability and cost-efficiency of current nuclear systems and encompasses a wide range of research areas, including advanced sensor development for harsh environments, on-line condition monitoring and condition-based maintenance, and human performance in advanced control systems. This research area is evolving from INL's rich 55-year legacy in nuclear reactor design, reactor demonstration, reactor operations, and reactor safety, which has resulted in the design, construction, and operation of 52 nuclear reactors. Because of this expertise in nuclear systems, INL represents the U.S. to the International Atomic Energy Agency in I&C areas and leads ICIS research projects for U.S. customers, including DOE and the Nuclear Regulatory Commission (NRC).

In 1999, DOE Secretary Bill Richardson designated INL as the Lead Laboratory for Nuclear Technology Research.

On July 15, 2002, DOE Secretary Spencer Abraham stated INL "will be the central command center for the federal government's Generation IV nuclear systems research."

ICIS research will enable cost-effective upgrades of existing nuclear power plants, facilitate design and licensing of near-term systems and programs (e.g., Nuclear Power 2010), and result in the integration of synergistic systems into future programs (e.g., Generation IV reactor [Gen IV]) and very high-temperature reactor [VHTR]). Additionally, ICIS research enables interdependent, ongoing programs, such as the Advanced Fuel Cycle Initiative, the Hydrogen Initiative, and the Space Nuclear Program.

The nuclear plant life cycle (shown in Figure 10) covers a broad range of interrelated issues from design inception to decommissioning. ICIS is an integral component of each element of this life cycle. For example, the ICIS systems for next-generation nuclear plants must monitor the health of energy production; provide sensors and systems to detect proliferation activities; balance plant transmission and safety systems; establish the risk basis for design and licensing processes; and provide assurance that the systems will be maintained within the licensing basis of the plant.

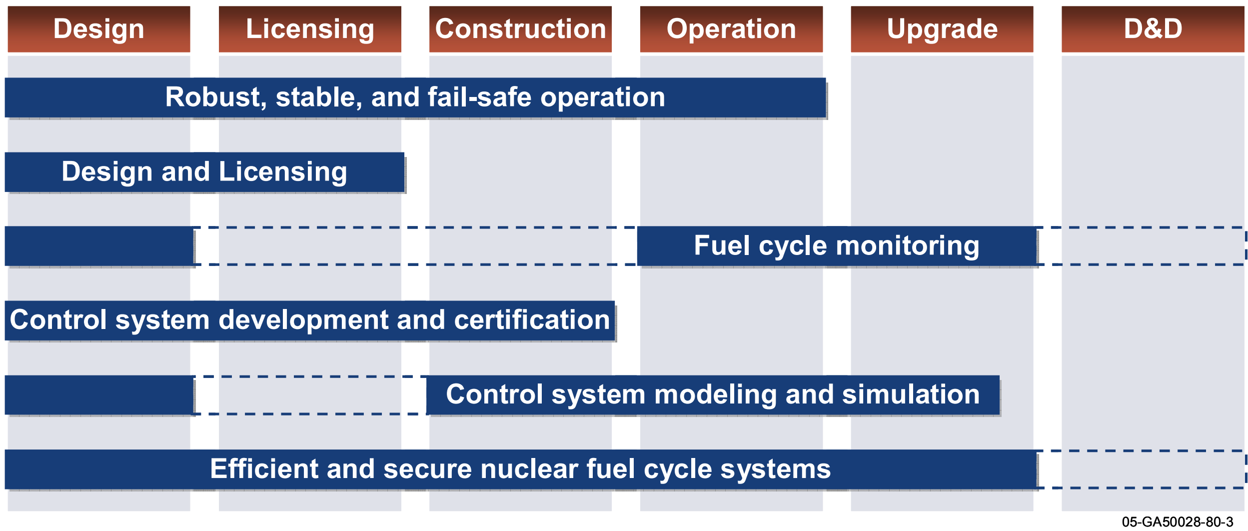


Figure 10. ICIS is an essential component of all elements of the nuclear plant life cycle.

By focusing on all phases of the nuclear plant life cycle, ICIS nuclear energy and nonproliferation research will:

- Increase plant reliability
- Provide strategies for new plant design and licensing
- Monitor fuel cycles
- Develop and test control systems
- Model and simulate plant and control systems
- Provide efficient and secure nuclear fuel cycle systems.

Increase Plant Reliability: Robust, Stable, and Fail-Safe Plants

High reliability and cost efficiency are vital to attracting investment and renewing growth in nuclear power generation facilities. ICIS will enable synergistic process control, providing efficiency in nuclear power operations that is key to achieving reliability and cost effectiveness.

Because sensors and controls will be deployed in harsher and harsher operating environments, research is needed to produce sensors that can provide new capabilities while functioning reliably in these environments (e.g., high temperature, highly corrosive, and high radiation). Sensors and controllers must be designed not only for anticipated conditions, but must also be capable of functioning beyond foreseeable accident conditions. Control systems with a secure network of sensors and controllers must employ control strategies that are intrinsically capable of ensuring plant safety and security across a range of accident conditions. Such demands require designs that explicitly account for failures and directly incorporate survivable and reconfigurable system control strategies. Software design of process control systems must emphasize the critical safety and operability aspects of system performance and be designed to be used by plant personnel.

Provide Strategies for New Plant Design and Licensing

Although current systems must be capable of complying with standard criteria for Class 1E Power Systems for Nuclear Power Generating Stations (IEEE-STD-308, 2001) and a host of other standards, new standards will also be needed to certify next-generation plant designs and the technical bases to support licensing.

The NRC plans to develop "technology-neutral" licensing requirements for advanced reactors. This requires that several steps be taken to support efficient licensing:

- Review the current regulatory framework for licensing of advanced energy and ICIS systems
- Conduct a gap analysis to determine the technical basis needed to support amendments or addendums to the regulatory framework
- Develop technical bases to support changes
- Develop new standards and regulations that permit specific changes.

To advance technology-neutral licensing related to instrumentation, control, and human factors, the following actions should be taken through a joint research program involving a DOE, NRC, industry, and the university consortium:

- Review experience gained from development, implementation, maintenance, and reliability of modern ICIS systems, especially those employing digital technologies at power generating stations
- Develop risk models for advanced ICIS systems
- Develop a gap analysis to determine the ICIS safety, security, and reliability requirements for next generation nuclear reactor operation, thus, providing a basis for the R&D path forward
- Review and compare advanced control and information systems for advanced reactors with those for conventional reactors to assess the safety-significance and basis for licensing of new plant design(s)
- Study the role of human operators in advanced plant designs to establish the basis for use of automation
- Assess staffing requirements for advanced plant resources, including control room personnel, non-licensed facility personnel, and operating organizations
- Guide human-system design to promote design and licensing of hybrid and digital systems for advanced plants.

Monitor Fuel Cycles

As the different elements of the nuclear fuel cycle (e.g., enrichment, fuel fabrication, reactors, reprocessing, and waste disposal) become more closely integrated with each other, a synergistic approach is necessary to better manage overall operation and meet requirements such as enhanced safety, competitive economics, improved proliferation resistance, and minimal waste generation.

Monitoring all nuclear fuel cycle constituents is critical and requires the deployment of complex system architectures consisting of distributed sensors, actuators, controllers, and decision-making processes. As these components need to communicate with each other, the development of reliable and secure data transmission technologies is important. For example, implementation of secure wireless communication is expected to return important savings and provide greater flexibility during both deployment and operations. Similarly, under a synergetic ICIS strategy, it is crucial to maintain an adequate situational awareness of the state of the overall system and each of its constituents.

Continual online monitoring of system state and health is important, not only to operate advanced nuclear fuel cycles efficiently and economically, but also to provide indicators of proliferation activities. Operators must be able to promptly discover anomalies that may compromise safety, security, and process integrity, and they must also optimally schedule maintenance activities; thus, a new generation of sensors is critical for monitoring all aspects of the fuel cycle.

As proliferation is an ongoing issue associated with the nuclear industry and the development of weapons of mass destruction, new non-proliferation ICIS technologies and sensors are needed. These technologies must ensure a sustainable strategy to ensure nuclear process transparency and to detect facility misuse. Improved identification and traceability of equipment and personnel associated with nuclear systems will also contribute to these transparency and proliferation-prevention goals and support the INL fuel cycle initiative, SINEMA.

Develop and Test Control Systems

INL possesses a substantial R&D background in the operation and evaluation of nuclear control systems. Our research expertise includes quantitative analysis of risks, development of real-time control system prognostic systems, and control system evaluation to establish resilience to cyber threats. Expertise in nuclear control systems is essential for the Gen IV program, but also supports the Nuclear Power 2010 program and current nuclear power plant operating and upgrade decisions.

Controls and the associated sensor systems provide an intricate network of data flow and control signals to operators who monitor and direct system operation. This system also involves complex software architecture; thus, software reliability and digital I&C reliability assessment are essential to plant operations, as well as to the design process.

Thus, as system functionality advances, the complexity of such systems reduces our ability to fully understand and quantify the risks of operation under all circumstances. Research is needed at all stages, from design to decommissioning, as shown in Figure 10, including areas such as design validation and real-time operational assessments of digital control systems. The following concepts support the need for this ICIS research:

- The failure of digital I&C systems is shown to have an impact on nuclear power plant performance (Brill 2000)
- An increased reliance on digital systems and automation will be required to support a “100-person” plant

Nancy Leveson (2004) of MIT’s Aero/Astro Software Engineering Research Laboratory states the following about the development of complex systems: “We are designing systems with potential interactions among the components that cannot be thoroughly planned, understood, anticipated, or guarded against. The operation of some systems is so complex that it defies the understanding of all but a few experts, and sometimes even they have incomplete information about its potential behavior. Software is an important factor here: it has allowed us to implement more integrated, multi-loop control in systems containing large numbers of dynamically interacting components where tight coupling allows disruptions or dysfunctional interactions in one part of the system to have far-ranging rippling effects. The problem is that we are attempting to build systems that are beyond our ability to intellectually manage: Increased interactive complexity and coupling make it difficult for the designers to consider all the potential system states or for operators to handle all normal and abnormal situations and disturbances safely and effectively.”

- Testing and design validation methods are essential, but cannot account for all the complex real-time interactions and potential failure of hardware, software, and human systems within these control systems
- A defense-in-depth and diversity (Chapter 7, NUREG0800, BTP-19, 1997) approach is necessary to anticipate and mitigate the effects of potential system failures to optimize plant efficiency, maintain high availability, and ensure system safety margins.

Model and Simulate Plant and Control Systems

Next-generation nuclear power plants, particularly if coupled with large-scale hydrogen production (as shown in Figure 11), present unique design, construction, and operational challenges. Advanced sensors, instrumentation, and measurement systems, coupled with greater levels of automation and prognostics, are required to achieve the "100-person" plant envisioned for the future nuclear power plant operation. Furthermore, because revolutionary ICIS technologies will allow new ways of operation not yet considered in traditional probabilistic risk analysis, research is needed to inform risk-based development and operations decisions. The development of comprehensive models and the application of simulation are key elements in the design and validation of new technologies and operating concepts.

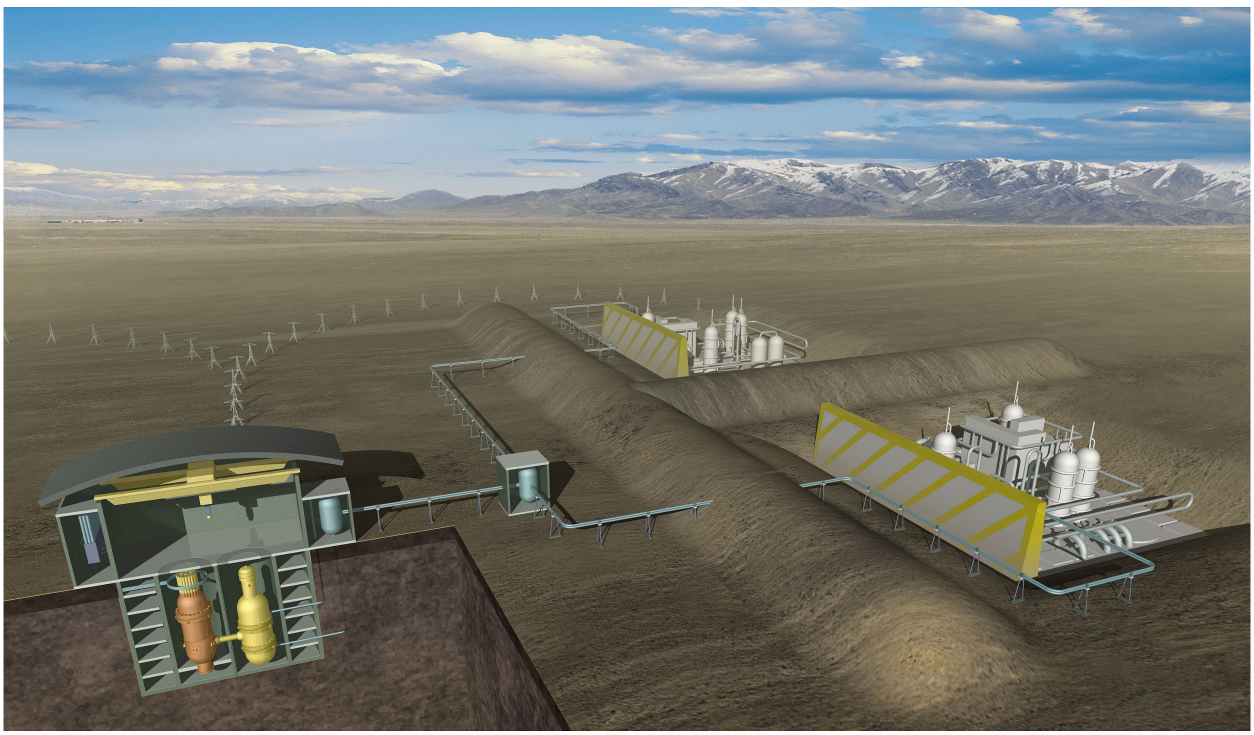


Figure 11. Automation and synergistic systems are essential in next-generation reactors like the VHTR that will generate power and hydrogen to meet U.S. energy security needs.

Modeling and simulation capability and facilities, including a re-configurable Nuclear Power Plant Control and Simulation user facility, are required to support component evaluation, system evaluation, and joint system integration for next-generation ICIS concepts. No such national research facility currently exists. The need for a nuclear control room simulator and simulation studies were cited as a needed research component by the NRC Advisory Committee on Reactor Safeguards (September 2002), as well as by the Department of Energy IC&HMI Working Group (May 2002).

To address the need for modeling and simulation user facilities, INL will provide leadership in three major areas:

- Component evaluation - control system models to evaluate new sensors, e.g., high temperature thermocouples, and transmission systems, including wireless systems
- System evaluation - control system models, mockups, and simulators to evaluate new control system operating concepts, such as prognostics and automation
- Joint system evaluation - control system facilities to support the evaluation of joint human machine operations and, particularly, human performance.

Research in these areas will leverage INL's longstanding history in nuclear reactor design, development, and testing, as well as in basic nuclear science research. The user facilities will enable not only research, but also development of the operational expertise that is needed for field deployment of research systems. The value of user facilities is evident in the Advanced Test Reactor (ATR) simulator training facility, operating for 30 years. This simulator allowed ATR to achieve a new record for the longest uninterrupted operating period in its 36-year history—57.35 days; nearly the maximum possible operating period based on ATR's fuel loading and power level.

User facilities are needed to enable next generation nuclear control designs as stated in "DOE NP2010 Construction Schedule Evaluation" (2004). "Digital control designs for the main control room and plant simulators are also omitted or loosely defined within the schedules. Because the simulator is required for operator training, and operators are needed for plant testing, these activities could impact critical path. Additionally, the United States (U.S.) regulatory requirements that will be placed on new digital controls are largely untested. This raises the risk of schedule increases."

The need exists for a next-generation nuclear plant user facility to evaluate the effect of new ICIS technologies and information presentation concepts on human performance. The user facility will provide qualitative and quantitative data to not only support design decisions, but also to provide risk data to facilitate an informed licensing process. These data will help provide Nuclear Power 2010 and Gen IV vendors with a design basis for defining specific aspects of control room operation.

Provide Efficient and Secure Nuclear Fuel Cycle Systems

Support is needed to establish research and analysis facilities to evaluate competing designs against acceptance criteria and to identify approaches that emphasize lower cost and better proliferation resistance and waste management practices. For proliferation resistance, there is also the need to develop integrated safeguards and proliferation-detection solutions to effectively address the challenges imposed by the vast amount of sensory data that will be generated by modern, large-scale nuclear facilities. The volume and diversity of these data make the task of ensuring safeguards compliance challenging and highly complex.

Traditionally, safeguards design efforts are often conducted ad hoc and do not exploit the known dynamic relations that exist among system components. Consequently, to compensate for uncertainty regarding facility operations and possible nuclear material diversion paths, current design strategies can lead to overly conservative instrumentation approaches. This over-design strategy may lead to excessive instrumentation and operation costs, without necessarily improving safeguards effectiveness. Deploying cost-effective solutions requires an integrated, synergistic safeguards strategy that embraces the notion of real-time operations process integrity and strengthens traditional, near-real-time, material accountancy techniques.

The advantages of various nuclear fuel-cycle options should be measured and evaluated holistically. The anticipated roles, merits, and limitations of specific reactor design concepts should be considered in design selection. To this end, there is the need to establish a comprehensive, overreaching framework for the modeling, simulation, and evaluation of commercial nuclear systems. Large numbers of alternative concepts and what-if scenarios can be investigated to compute system sensitivities to specific criteria, including costs, safety, waste management, and proliferation resistance characteristics. To quantify and compare results, appropriate metrics must be developed. Results from these analyses will be used to discover process inefficiencies, suggest remedies, identify technological gaps, and prioritize development efforts that will provide the greatest returns. This virtual development and prototyping framework will provide nuclear industry stakeholders with direct visibility into system performance, engineering risk, and critical evaluation drivers.

Path Forward for Nuclear Energy and Nonproliferation Systems

For ICIS to enable the next generation of synergistic instrumentation, control, and intelligent system strategies for nuclear plants and fuel cycles, focused research is required as shown in Figure 12.

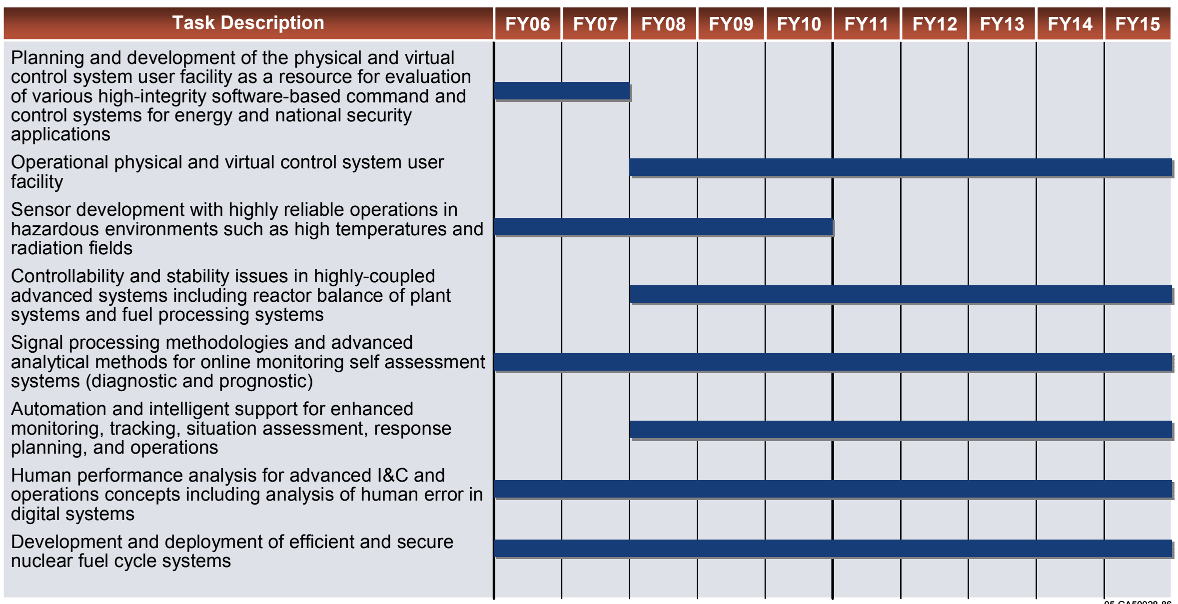


Figure 12. Nuclear energy and nonproliferation systems timeline.

Industrial Process Monitoring and Control

Applications for revolutionary instrumentation and controls include energy production and distribution systems, materials processing, transportation systems, oil and gas production systems, agricultural systems (see Figure 13), and various manufacturing processes. Using advanced process monitoring and control in industrial processes will allow plants to operate closer to the plant design point by reducing measurement uncertainty, as well as implementation of condition-based maintenance strategies. The ability of sensors and controls to recognize and adapt to the health of plants will allow significant increases in plant efficiency, lifetime, reliability, and safety. Thus, INL R&D work on ICIS for industrial process monitoring and control will support the needs of several DOE Program Offices, including Civilian Radioactive Waste Management, Energy Efficiency and Renewable Energy, and Fossil Energy.

Figure 13. Combine incorporating an advanced control system developed by INL increases grain harvesting efficiency of Idaho farmers.

Provide Systems with High Level of Awareness

Future control of general industrial processes should incorporate multilevel optimization, robustness in the face of disturbances and plant uncertainties, and the ability to operate a plant as well as safely shut down a plant in an impaired configuration. The control system should have a high level of awareness of both the process state and plant health. It should incorporate inherent protection that prevents an operator from accidentally or deliberately damaging the plant or operating the process in an unsafe manner. Individual components of complex systems should have sensors incorporated that can provide cradle-to-grave, real-time, status reports on the health of the component. Additionally, sensors should provide a measure of confidence in the data obtained, validation of their calibration and health, and interpretation of their data. Communications between various functional elements of the control system should employ plug-and-play interfaces and automatic identification of system configuration. The operator interface should incorporate high-level, plain-language commands, voice recognition capabilities, and bi-directional human/control system communications. The control systems should incorporate open architecture hardware and software standards, and commercial off-the-shelf hardware.

INL is developing a set of technologies that enable a materials processing or manufacturing system to measure the quality of a product as it is being processed. The results of the quality measurements are fed into a lifetime prediction model and used to assess the expected future life of the product. Process control parameters can then be optimized, obtaining increased product lifetime.

Develop Revolutionary Monitoring and Control Tools

Revolutionary advances in instrumentation and controls technologies will require several major scientific and engineering research breakthroughs. Contemporary controls technology is founded on control theory that is based on lumped parameter, linearized, ordinary differential equation dynamic models. Research is needed on stability theory for distributed, non-linear, dynamic systems with control algorithms for associated partial differential equation models. Machine learning, knowledge discovery, and complex system theory need to be developed far beyond today’s understanding of these topics.

Research is also needed on natural language, linguistic interfaces, and algorithms for object detection, recognition, and significance classification in advanced sensors. Novel feature recognition research is also needed to support intelligent sensor development and formulation of advanced decision-making algorithms. Dynamic models of complex plants are needed, including reactor systems, energy distribution systems, and various manufacturing and materials processes. Solution of these models in a real-time control system will require significant advances in computational methods, including fast solution algorithms and miniaturized cluster computers suitable for embedding directly into plant control systems. Finally, computational intelligence methods, including artificial neural networks, evolutionary computation, and fuzzy logic need theoretical bases that include the ability to capture the process and plant physics-governing dynamic behavior. Such capability will support development of sensors and controls that can recognize the state and health of processes and plants undergoing both gradual and abrupt changes in health and configuration.

Path Forward for Industrial Process Monitoring and Control

To support industrial process monitoring and control research, design and operation of user facilities and building collaborations are critical as shown in Figure 14 .

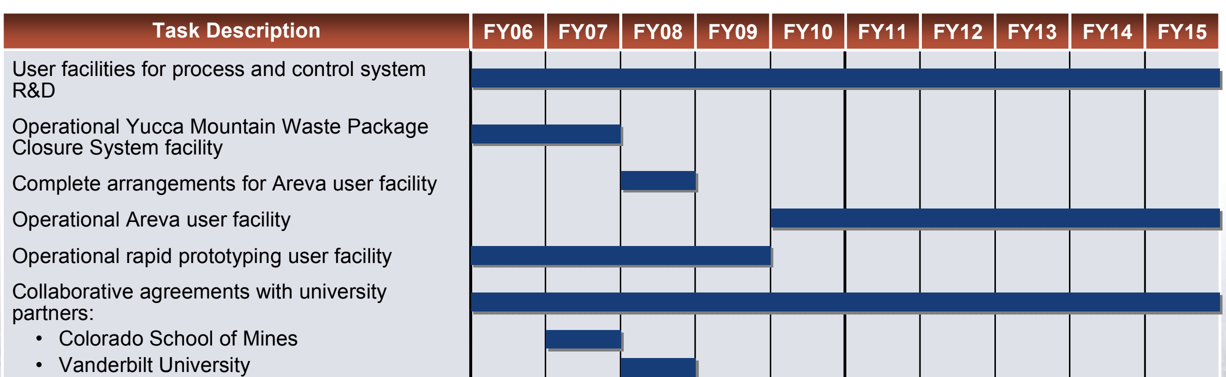


Figure 14. Industrial process monitoring and control timeline.

Threat Detection and Mitigation

The effectiveness of a security program for protecting the nation's critical infrastructure will depend on a quantifiable prioritization of safety and economic concerns, based on the risk associated with a control system being compromised. Many industries, including utilities, oil and gas, and chemical, depend on complex monitoring and control systems to maintain the economics of their business and to ensure the safety of their employees and area residents. With the increased focus on national and homeland security as a result of the September 11 terrorist attacks, INL leveraged its 55-year history in developing, operating, and maintaining complex control systems to be a key player in the protection of critical infrastructure.

Building on this base, INL established the Critical Infrastructure Test Range (Figure 15) to test security and cyber systems developed to protect the nation's infrastructure against attacks from hackers, virus writers, disgruntled employees, terrorist organizations, and nation states. The test range allows security evaluation and testing of full-scale infrastructure systems, providing live testing of an operating plant process or installation in a controlled environment to determine weaknesses and recommend solutions. The test range covers the many facets of computerized monitoring and control, and includes the SCADA Test Bed, the Control Systems Security Center, the Wireless Test Bed, the Cyber Security Test Bed, and other testing facilities in the areas of physical security, infrastructure testing, and contraband detection.

Figure 15. INL facilities representative of the nation's critical infrastructure.

Develop Next-Generation Physical and Cyber Security Tools

ICIS threat and mitigation research objectives are designed to protect the nation's infrastructure in the areas of physical and cyber security. These objectives include:

- Risk prioritization and graded implementation
- Proactive detection, mitigation, and response
- System design
- Corporate roles and responsibilities for control systems security
- Sensor detection applications to physical security.

Risk Prioritization and Graded Implementation

To reduce operating cost and increase flexibility in the implementation of control systems, control system vendors have moved to open systems architecture and industries have implemented distributed monitoring and control. However, evaluations performed after the September 11 attacks made the vulnerability of these systems evident, prompting a thorough review of the security risks associated with each implementation. A presidential directive (HSPD-7) for homeland security has provided risk criteria, and in response to its homeland security mission, INL has proposed quantifiable prioritization levels. Once these levels are adopted, they will form the basis for development of a graded, or layered, approach to the rigor of security monitoring and detection performed on an individual control system. The combination of the prioritization and layered techniques, in turn, forms the basis for standards development and metrics, where maintenance and enhancement can be maintained with changing control system architectures.

Proactive Detection, Mitigation, and Response

Proactively recognizing, mitigating, and responding to a potential threat before a control system is compromised is key to ensuring system integrity. While there are tools available that are aimed at preventing undesired intrusion and corruption of data, these systems are reactive in nature. A unified approach to proactively protecting the various systems architectures requires the development of modeling techniques that characterize threat dynamics for control system security. These threat dynamics play a pivotal role in characterizing the nature of the threat and allow the development of response scenarios.

System Design

While much of the implementation of security measures for control systems has depended on dedicated devices that are part of information technology systems, including networking devices and server-based firewalls, security measures that are implemented within the control system components have been limited primarily to password protections and privileges built into the HMI. These measures may no longer be adequate to mitigate threats. Until vendors understand the multifaceted nature of security protection, it will be up to government institutions to characterize security issues and develop solutions which, if implemented as part of the control system package, will mitigate the security issue. Redundant design, once only used to accommodate electronic component or component design failures, should consider security aspects. Technologies will need to be developed that enable security detection and response to be incorporated in control system designs.

Corporate Roles and Responsibilities for Threat Detection

The interactions and segregation of responsibilities between physical, cyber, control system, and operations personnel responsible for aspects of security can often dictate the promptness and effectiveness of a response to a control system compromise. While the development of proactive technologies and the embedding of security into the control system can provide the most effective response, human interaction in the current corporate atmosphere is a weakness and requires a synergistic approach to ensure the security of existing systems. An evaluation and modeling of the nation's corporate infrastructure for security protection should be completed, and a corporate matrix that identifies vulnerabilities in the identification and response should be developed.

Sensor Detection Applications

Unique and revolutionary sensor detection methods are required to ensure the security of the nation's utility infrastructure, ports of entry, and other public facilities. As the communications and power distribution systems are spread through many remote locations, they are especially susceptible and require sensors to detect and prevent tampering. Our economy and its health depend on the free flow of goods through our nation's ports, but these facilities also provide a potential access point for entry of explosive devices and other tools of terrorism. With the sheer amount of goods that enter this country, not to mention the multiple types of devices that are of concern, application of these sensors to existing transport processes using varied approaches to measurement is required.

Path Forward for Threat Detection and Mitigation

To ensure the nation's infrastructure requires actions that build on the existing capabilities at INL. Although initial measures must be prescriptive, research is needed to ensure the infrastructure's future as the threats become more diverse and the adversary becomes technologically advanced. Figure 16 provides a timeline for the major research components of the threat detection and mitigation research area.

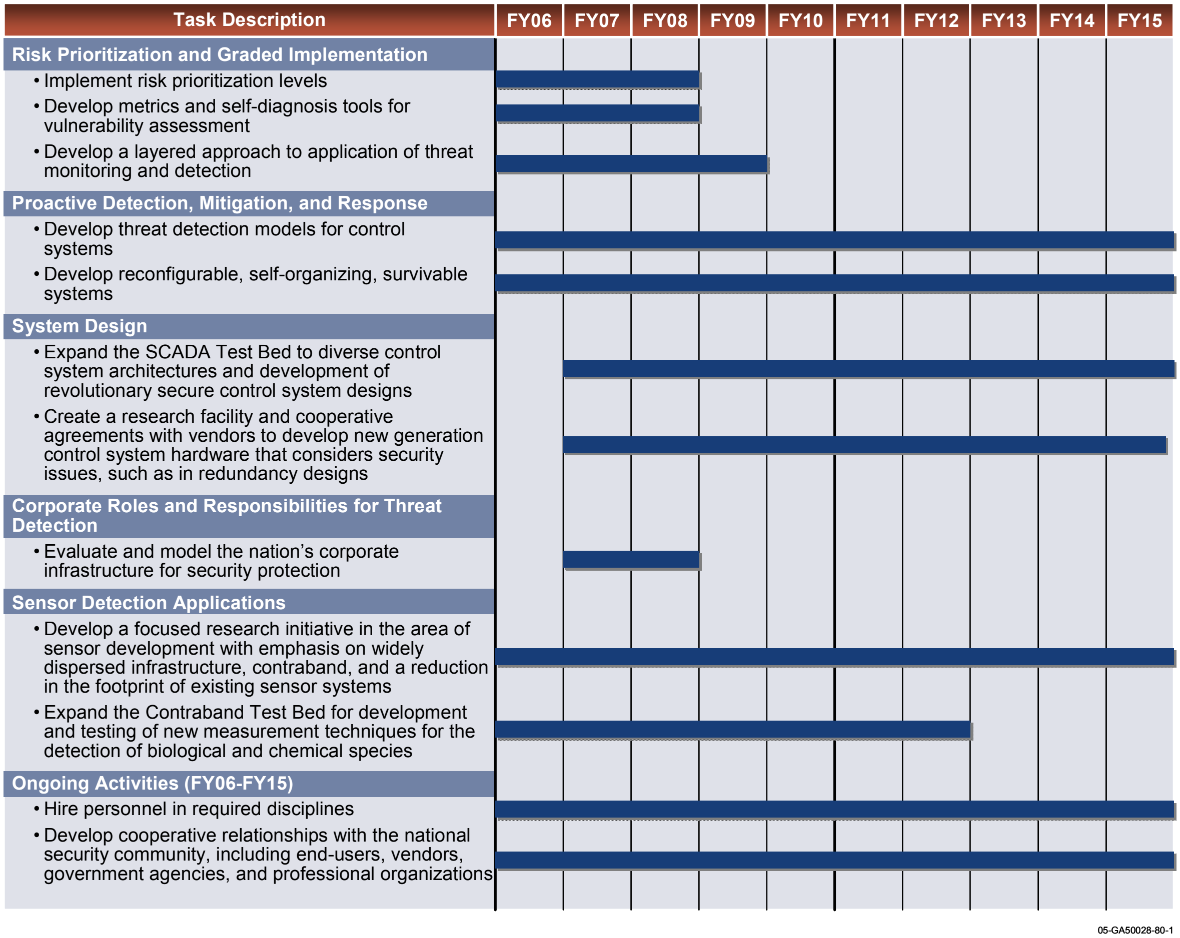


Figure 16. Threat detection and mitigation timeline.

Autonomous and Semi-Autonomous Robotics and Intelligent Machines

From the exploration of outer space to the ocean's deepest depths, robotic systems are playing a more and more important role in exploring and working in harsh, hostile, and "human unfriendly" environments. Today's newest generation of intelligent machines and systems are providing unique capabilities across diverse settings that were unimaginable even a decade ago. Tethered, remotely-operated vehicles are important in the oil industry's bid to produce ever greater amounts of oil from ever greater depths of water. Remote robotic systems enable DOE to handle radioactively contaminated materials safely and securely, and a whole array of next-generation air, ground, and water robots will aid the Department of Homeland Security and other emergency-response agencies in dealing with disasters faster, more safely, and more effectively.

Robotic air and ground vehicles are also significantly enhancing current military operational capabilities. UAVs have proven particularly useful as persistent intelligence, surveillance, and reconnaissance assets, especially in the detection of time-sensitive targets. Unmanned ground vehicles (UGVs) enable explosive ordnance disposal technicians to investigate and destroy improvised and other types of explosive devices from safe, stand-off distances. Additionally, as naval forces enter and fight in the shallow-water littoral or, "brown water" zone, autonomous underwater vehicles will play a critical role in detecting and destroying sea-laid mines prior to naval force entry.

Despite such advances, significant technical challenges remain in the area of robotics and intelligent systems. Chief among these challenges are the three I's: intelligence, integration, and interaction. INL's robotic and intelligent system capabilities are well positioned to meet these identified challenges.

Provide Robotic Systems with Intelligence, Integration, and Interaction

Intelligence

Traditionally, most robotic systems have derived their "intelligence" from commands input by a human operator through a tele- or remote-operational interface. As robotic systems take on more complex roles and tasks, on-board intelligent processing capabilities, encoded with an array of embedded behaviors, will become mandatory. Such behavior-based intelligence capabilities will enable enhanced platform mobility, allowing robotic systems to autonomously sense, map, and traverse unstructured environments without the need for *a priori* maps or human-directed guidance. Additionally, onboard intelligence kernels with rich behavior-based libraries will allow robotic systems to autonomously and semi-autonomously affect and physically manipulate their environment in completely new and novel ways. These derived intelligence-based mobile manipulation and mobility capabilities will form the basis for a whole new class of intelligent mobile platforms—platforms that can be independently configured to perform a diverse array of tasks under varied operational conditions.

Accordingly, and regardless of specific domain or application area, a common and platform-portable intelligence "kernel" will form the basis for next-generation robotic systems, as shown in Figure 17. By leveraging current work in this area, INL is in a unique position to be at the forefront of robotic intelligence development and implementation.

Figure 17. INL's intelligence kernel uses a wide range of capabilities to implement ICIS in robotic systems.

Integration

A second critical need is to integrate diverse robotic air, ground, and water platforms into a single, integrated, operational system, one capable of carrying out mission-needed tasks in an intelligent, collaborative, and cooperative manner. Platform-common communication, command, control, and interface protocols and associated technologies will be required to integrate diverse unmanned and manned systems seamlessly into a single, functional, operational system. INL's unique UAV/UGV capabilities and physical assets associated with its remote, unmanned system research park will enable the laboratory to become a highly valued basic and applied research, development, and experimental testing center.

Interaction

As robotic systems become more intelligent, they will be viewed as valued team members in mixed human/robotic team settings. In such proximal team-based environments, it will become vital to develop enabling technologies that allow for more natural human/robot interaction without the need for the cumbersome intervening interface devices used today. The ability to plan and coordinate human and robotic tasks is an additional critical need. Combining its demonstrated expertise in robotics and human factors, INL will provide high-value research and technology development in this new and emerging area of human/robot teaming, interaction, and collaboration.

Enhance Robotic and Intelligent Systems for End-Use Applications

By successfully overcoming the technical challenges associated with intelligence, integration, and interaction via the creation of a core set of platform-portable, intelligent, and behavior-based technologies, INL will be able to greatly enhance robotic and intelligent system use, irrespective of operational setting or required platform/system configuration. Such new capabilities will meet the requirements and needs of a diverse user set, as shown in Table 2.

Table 2. End users' specific needs for robotic and intelligent systems.

End User	Autonomous and Semi-Autonomous Robotics and Intelligent Machines Needs
DOE	Develop system to replace manned or tele-operated robotic systems for use in high radiation and other hazardous work environments Reduce and, in many instances, eliminate human exposure to adverse environmental conditions while significantly increasing overall operator and operational performance, safety, and productivity
National Aeronautics and Space Administration	Develop intelligent robotic systems, including self-healing intelligent control systems, to enable robotic ground vehicles that can autonomously initiate actions without the need for earth-generated signals Develop embedded intelligent systems that can provide autonomous, effective management of varied on-board systems, including energy and propulsion systems.
Department of Defense and Department of Homeland Security	Provide research and technology development to permit many new capabilities, ranging from the development of self-configuring and dynamic sensor networks to a compatible robotic soldier "assistant" that can execute a number of tasks both independently and in support of human-issued commands Provide better mission integration and execution of diverse robotic platforms Increase security of our own national borders by the continuous deployment of improved air and ground robotic- and intelligence-based sensor arrays

End User	Autonomous and Semi-Autonomous Robotics and Intelligent Machines Needs
Ocean exploration	Assist in deep (>1,000 ft) and ultra deep (>5,000 ft) offshore oil exploration and production efforts by eliminating the need for tethered or "cabled" remotely-operated vehicle systems Remove the requirement for expensive, dynamically-positioned support vessels Enable exploration and mining of the deep ocean's biological and mineral resources in totally new and environmentally sensitive ways
Mining and other bulk-handling operations	Revolutionize the handling and transport of bulk materials in semi-structured environments Improve the safety and productivity of operations from hauling ore in open pit mines to moving bulk cargo by the use of intelligent, autonomous robotic systems

Path Forward for Autonomous and Semi-Autonomous Robotics and Intelligent Machines

If we are to achieve greater safety, utility, applicability, and productivity from next-generation robotic systems, the technical challenges of intelligence, integration, and interaction must be successfully addressed. Ongoing work in ICIS at INL will provide a firm foundation and springboard for this critical scientific research and technology development endeavor. To successfully meet these challenges, a series of INL-specific future enabling milestones must be met (see Figure 18).

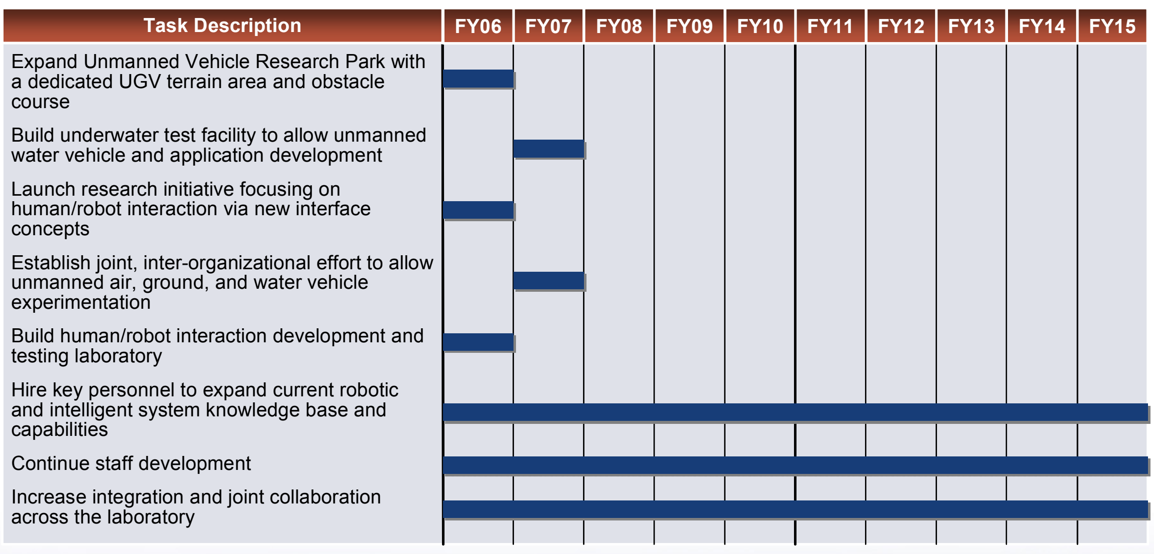


Figure 18. Autonomous and semi-autonomous robotics and intelligent machines timeline.

Human-Centric Interfaces and Controls

The system operator is an integral part of the system and must be strongly considered in the design. Too often, designers are successful in their attempt to remove the human from the loop, leaving the operator devoid of information essential to resolving unexpected situations. To build systems that are highly reliable, operators must be central to the design to optimize their performance and to maximize the human's capabilities.

Our research will revolutionize human-machine interaction by developing the means to exploit human biology and psychology as a basis for new human-machine systems.

To be successful and optimize performance, ICIS systems must take into account how humans learn, process information and, ultimately, make decisions. As shown in Figure 19, command and control operations are an excellent example of an application in which this type of integration of instrument, controls, and human is essential for success. Our research will revolutionize human-machine interaction by developing the means to exploit human biology and psychology as a basis for new human-machine systems.

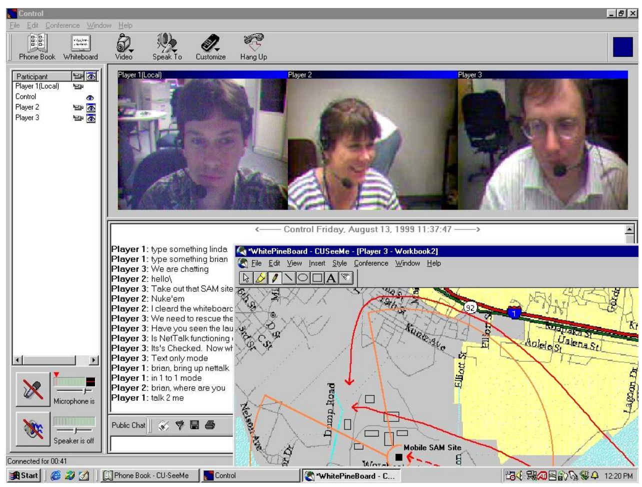


Figure 19. ICIS strategies are essential for command and control operations.

The concept of human-centered design began in the last decade when it became clear in the aviation industry that designers of aircraft were implementing "automated" systems that caused pilots to lose situational awareness (Billings 1991). The clumsy automation resulted in the loss of pilot situational awareness, such that the pilot did not understand or necessarily agree with the flight control actions being taken by the system. Early on, pilots would simply turn off the automated systems in favor of manual control.

ICIS challenges the paradigm that, "The basic rules of [human-computer] interaction are the same as they were in the days of the ENIAC [Electronic Numerical Integrator and Computer]: users must engage in an explicit, machine oriented dialogue with the computer rather than interact with the computer as they do with other people." (Cooperstock et. al.)

Since somewhere between 60 and 80% of all industrial accidents are caused by human actions (Gertman and Blackman 1994), an unacceptable condition results. Research and anecdotal findings show how designers of automated control systems can introduce the potential for error, or at least a significant loss of operator confidence in the system.

Build Interface Channels between Humans and Machines

Future interface systems will rely to a greater extent on multiple interface channels between human and machine systems, both for display and control. Sensory and perceptual channels will be exploited to a greater extent. Devices such as haptic, visual, auditory, and gesture control interfaces; topographic and holographic displays; and immersive, synthetic environments will become more prevalent. Designers will encounter problems for which there are no standards, empirical data, advanced concept demonstrations, prior experience, or organizations with the knowledge to support the selection of different technological alternatives.

The already tight coupling between human reliability and system performance will increase in these systems, especially in environments such as military and space command centers where the tempo of activity and criticality of actions and decisions are already great.

The design, development, and deployment of such systems cannot afford developmental testing or concept validation in the field, where the consequences of errors and other failures are high. Testing of such systems will increasingly rely on modeling and simulation and controlled tests and evaluations. The revolutionary nature of such technologies will dictate the development of new methods and techniques for their testing and the measurement of human and system data to demonstrate effectiveness prior to fielding.

Path Forward for Human-Centric Interfaces and Controls

By linking diagnostics, prognostics, and human interfaces, we can substantially improve the overall efficiency and reliability of systems. Research is needed to take advantage of the potential improvements in these systems. For example, research is required to:

- Determine what kind of instrumentation and control strategies would best support decision-making in loss-of-offsite-power scenarios
- Better understand how data fusion can support the integration of information for crews in diverse applications, including nuclear power plants, airplanes, and battle field command operations
- Understand how control systems can be adapted to different levels of operational expertise
- Develop intelligent methods for the display and prioritization of process and prognostic alarms
- Increase the operator’s situational awareness to improve performance, safety, and productivity
- Develop human-machine interfaces, natural language interfaces, and bio-based interfaces that complement the human and do not present unnatural ways of interacting with systems or prevent a complete understanding of the systems.

Operator system awareness can also be improved through advanced instrumentation and control methods that support system-related (what it is doing now), predictive (what it might do), and response (what the operator should do) descriptions. In addition, operator system awareness can be improved through automated knowledge discovery systems that interrogate the equipment to determine system status and deliver that information to the operator in the best possible way.

Error must be reduced, but so must the ease of error recovery. More flexible control and computational system architectures that can overcome system reconfiguration will be needed.

Additional research must be conducted in the areas of:

- Natural human interfaces
- Systems to support increased awareness in complex operational settings

- Advanced voice/visual recognition, processing, and feedback
- Adaptive control systems
- Natural language interfaces
- Test and evaluation of advanced human-centric systems
- Data to support risk assessment of these systems
- Metaphysical control.

The human-centric interfaces and controls research area crosscuts every other research area described in this roadmap. Wherever there is a human in the loop, research from this area must be considered. The timeline, shown in Figure 20, has been established to achieve this area's identified goals.

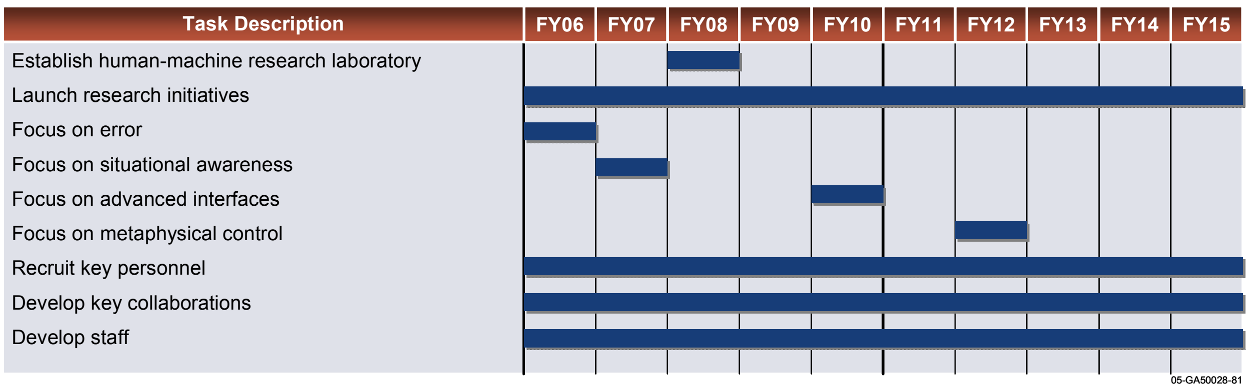


Figure 20. Human-centric interfaces and controls timeline.

STRATEGY

Our strategic approach will have six overarching thrusts that support the ICIS nexus elements and the ICIS research areas.

- Create and foster highly innovative R&D capabilities to meet our customer needs
- Design and operate user research, test, and experimental facilities
- Recruit, retain, and develop exceptional staff
- Work collaboratively with INL Center for Advanced Modeling and Simulation, regional, national, and international research organizations
- Host a series of symposia focused on key research needs for ICIS
- Establish INL as the preeminent national and international center for ICIS research.

Create and Foster Innovative R&D

INL has comprehensive plans underway to revitalize ICIS R&D. This includes all aspects of the process: strategy, facilities, personnel, and investments. This scientific signature is one of those tools. Within the ICIS signature, we will specifically address the question of increasing creativity and innovation. We will look to building on the success of others and bring together multiple disciplines to spawn new ideas and thinking. We will focus our resources on creating this nexus of ideas from which to build.

Design and Operate User Research, Test, and Experimental Facilities

User facilities will be critical, not only to perform work, but also to build the right collaborations and address the major customer needs. This will require investments over the next 10-year period. These facilities will have diverse test environments to evaluate sensors, instrumentation, and controls, including:

- Designing and deploying a reconfigurable control room and process simulator to test new control philosophies and I&C systems
- Expanding the SCADA control test bed to include technologies that support the paradigm shift from “resist to attack” to “survive and adapt” in the development of secure control system designs
- Developing a laboratory to test unmanned systems with air, land, space, and water capability
- Establishing a robotic weld cell facility to support development of technology for Yucca Mountain waste package closure
- Establishing a robotic welding and inspection laboratory in collaboration with AREVA Corporation.

These facilities will require the ability to perform a wide variety of functions. Most notable is the ability to:

- Design and fabricate components using rapid prototyping for macroscopic models and structures (stereolithography), for microstructures such as microelectromechanical systems or custom integrated circuits, and for new computational systems
- Obtain equipment and develop advanced machining and manufacturing capabilities

- Collaborate with research partners over long distances and support distributed testing across multiple sites.

Recruit, Retain, and Develop Exceptional Staff

Recruiting top notch staff with experience in applicable research disciplines will also be a part of our strategic approach. We will focus on staff in the identified core areas of ICIS for nuclear energy and nonproliferation systems, industrial process monitoring and control, threat detection and mitigation, autonomous and semi-autonomous robotics and intelligent machines, and human-centric interfaces and controls.

These staff will necessarily be at a variety of levels. We will focus on the Ph.D. level, but we will also look for industry leaders who are thought and opinion leaders in ICIS. Also, integral to our success, is the high-caliber staff, including technicians that are required to execute this diverse work. We will also focus on retaining and developing the current workforce to build our own future leaders through mentoring and career growth opportunities. We will seek to demonstrate our commitment to this area and to our staff through appropriate investments in staff development. A staffing plan will be laid out in the next year to ensure the success of ICIS.

Build Collaborations with Regional, National, and International Research Organizations

Today there is no nationally or internationally recognized center for ICIS research as we have conceptualized it. We have the opportunity to seek out the best and brightest in these areas and to build research collaborations to establish and strengthen this center. We will go to the leading universities, both nationally and internationally. In addition, we will seek out the industrial leaders. Additionally, we will host a series of symposia focused on key research needs for ICIS.

A basic and essential building block for ICIS is advanced computing and modeling. We will, therefore, work closely with our own Center for Advanced Modeling and Simulation and request that they provide the following:

- Computational modeling techniques that enable interaction and visualization of the massive data sets that will be created by large sensor networks
- Comprehensive and collaborative virtual engineering methods (and desktop engineering tools) that integrate sensors, models, human interaction, and other key engineering process variables together for control system design
- Mathematicians to support research on methods of dealing with uncertainty and stability in the control of complex, distributed, dynamic systems
- Hardware and software infrastructure to support the creation of very large distributed plant models.

Build Capabilities for the Preeminent Center in ICIS

To support INL’s nuclear energy, national security, and energy security focus and assume an international leadership position in ICIS research requires capabilities in the following areas:

- Intelligent systems theory and algorithm development
- Control theory and algorithm development for Gen IV
- Advanced mathematical methods, including the self-determination of uncertainty
- Advanced methods for online condition monitoring and condition-based maintenance

- Human factors research and HMI development for the next generation of human synergistic control systems
- Sensor theory and hardware development for long–duration, extreme environments such as space, deep ocean, and high radiation
- Data analysis and object/feature/event/target recognition theory and algorithm development for intrusion detection, UAV applications, target recognition, and automated, real-time threat detection.
- Next-generation embedded hardware and software development for intelligent sensors and complex models for process control
- Next generation control system designs that consider safety and security aspects in the development of fail-safe controllers and sensors
- Experimental infrastructures where advanced decision systems can be demonstrated in realistic settings before they are deployed in actual systems
- Modeling and simulation of dynamic systems, nuclear/hydrogen power, balance of plant, coupled systems, and unmanned vehicle system mission planning and execution
- Systems design, integration, and prototyping for Gen IV, VHTR, and future combat systems
- Optics and electronics capabilities, including optical and quantum computing, optical fiber sensors, imaging devices, and multispectral measurements ranging over the entire gamut of gamma ray, x-ray, ultraviolet, visible, infrared, terahertz, microwave, and beyond.

ISSUES

The major issues facing this area are adequate staff, user research and test facilities, and partnerships. There is also an on-going need to sustain investments that support and enhance the ICIS infrastructure and staff. We need to actively recruit new scientists, engineers, and technicians at all levels. In doing so, it is incumbent on us to develop lasting relationships with the leading universities, research organizations (i.e., Center for Advanced Energy Studies), and industries in ICIS. In addition, we must seek the necessary capital resources to develop our facilities so that INL is the place to come to do leading-edge scientific research in ICIS. Partnerships must also be developed with industry to ensure the relevance of our R&D. This, in turn, should lead to the intellectual property that will further our reputation and funding to continue the development of this signature.

RECOMMENDATIONS

INL must take a very proactive stance internally to ensure that sensor and controls technologies are incorporated in advanced reactor and power generation systems. We also need to carry the message to DOE and other funding agencies that there is a need to address sensor and controls technologies early in the development of advanced reactor and power generation systems. In order to do so, the ICIS Science Signature workshop will become a permanent committee to coordinate ICIS activities within INL and to conduct related communications with DOE, Congress, and other government agencies.

INL should establish collaborative integration of the intelligent systems, robotics, human factors, and sensors and controls R&D programs at the laboratory to ensure that we give our customers the highest possible value in our products. To this end, we will establish major ICIS crosscutting activities that support nuclear energy, national security, and energy security goals as shown in Figure 21.

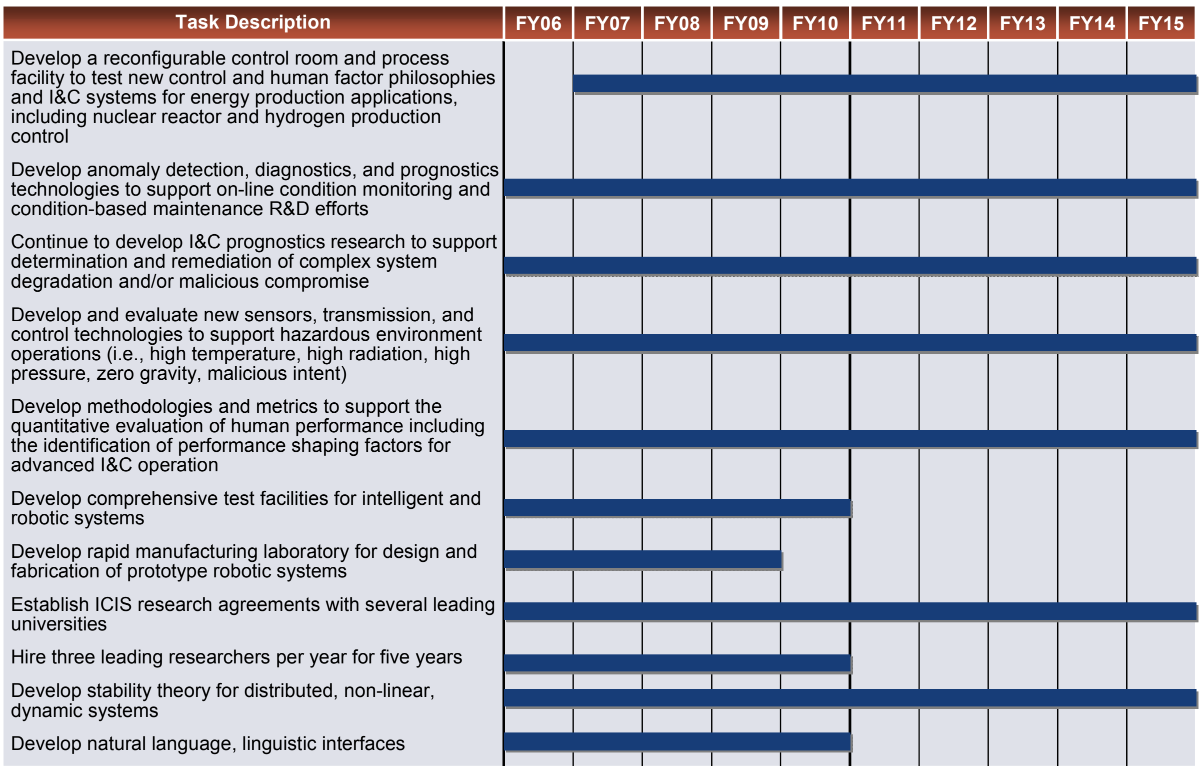


Figure 21. ICIS crosscutting activities timeline.

REFERENCES

Albus, James S., 1991, “Outline for a Theory of Intelligence,” *IEEE Transactions on Systems, Man, and Cybernetics*, Vol 21, No. 3, May/June 1991, pp. 473-509.

Billings, C.E., 1991, “Human Centered Aircraft Automation: A Concept and Guidelines,” NASA Ames Research Center, Moffet Field, CA: NASA Technical Memorandum 103885, August 1991.

Cooperstock, Jeremy R., Sidney Fels, William Buxton, Kenneth C. Smith, 1997, “Reactive Environments Commun.” *ACM*, Vol. 40, No. 9, 1997, pp. 65-73.

DOE, 2002, Instrumentation, Controls and Human-Machine Interface (IC&HMI) Technology Workshop, Gaithersburg, Maryland, May 2002, U.S. Department of Energy, p. 39.

Gertman, David I. and Blackman, Harold S., 1994, *Human Reliability and Safety Analysis Data Handbook,* New York: John Wiley-Interscience.

Leveson, N., 2004, “A New Accident Model for Engineering Safer Systems,” *Safety Science*, Vol. 42, No. 4, April 2004. Available online at: http://sunnyday.mit.edu/accidents/safetyscience-single.pdf.

Massachusetts Institute of Technology, 2003, “The Future of Nuclear Power: An Interdisciplinary MIT Study,” 2003, p. 14.

MPR-2627, 2004, “Construction Schedule Evaluation,” DOE NP2010 Revision 2, 2004, p. ix.

NRC, 2002, Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Human Factors, U.S. Nuclear Regulatory Commission, September 10, 2002, p. 215.