
Emerging Technologies in Instrumentation and Controls

Manuscript Completed: January 2003

Date Published: February 2003

Prepared by:

R. T. Wood, C. E. Antonescu (NRC), S. A. Arndt (NRC), C. L. Britton,
S. A. Brown-VanHoozer, J. A. Calvert (NRC), B. Damiano,
J. R. Easter (PLS), E. B. Freer, J. E. Hardy, L. M. Hively,
D. E. Holcomb, J. M. Jansen, R. A. Kisner, K. Korsah,
D. W. Miller (OSU), M. R. Moore, J. A. Mullens, J. S. Neal,
V. A. Protopopescu, R. A. Shaffer (NRC), J. C. Schryver, C. M. Smith,
R. W. Tucker, R. E. Uhrig, B. R. Upadhyaya (UTK), G. R. Wetherington,
T. L. Wilson (Georgia Tech), J. D. White, B. R. Whitus

Oak Ridge National Laboratory
Managed by UT-Battelle, LLC
Oak Ridge, TN 37831-6010

Christina E. Antonescu, NRC Project Manager

Prepared for
Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code Y6284

TABLE OF CONTENTS

EXECUTIVE SUMMARY	v
ACROYNYS	xiii
1. INTRODUCTION	1
1.1 Objectives of the Emerging Technology Survey	1
1.2 Research Approach for the Emerging Technology Survey	1
1.3 Scope of the Emerging Technology Survey	2
1.4 Structure of the Emerging Technology Report	3
2. STATE-OF-THE-ART DEVELOPMENT FOR I&C TECHNOLOGIES	5
2.1 Sensors and Measurement Systems	5
2.1.1 Silicon Carbide Flux Monitor	5
2.1.2 Solid-State Neutron Flux Monitor	6
2.1.3 Fuel Mimic Power Monitor	6
2.1.4 Scintillation-Based Measurements	7
2.1.5 Johnson Noise Thermometry	8
2.1.6 Ultrasonic Flowmeters	9
2.1.7 Magnetic Flowmeter for Measurement of Primary Coolant Flow	9
2.1.8 Fabry-Perot Fiber Optic Temperature Sensor	10
2.1.9 Optic Pressure Sensors	11
2.1.10 Gamma Ray Tomographic Spectrometry	11
2.1.11 Hydrogen Sensor	12
2.1.12 Smart Sensors	12
2.2 Communications Media and Networking	13
2.2.1 High-Performance Architectures	14
2.2.2 Network Physical Layers	15
2.2.3 Safety-Related Fieldbus	19
2.2.4 Network Security	23
2.2.5 Network Management	24
2.2.6 Network Design	25
2.3 Microprocessors and Other Integrated Circuits	25
2.3.1 Radiation-Hardened Integrated Circuits	26
2.3.2 System on a Chip	27
2.3.3 Optical Processors	29
2.3.4 Vertically Stacked Integrated Circuits	30
2.3.5 Nanotriodes	30
2.3.6 Microelectromechanical systems	30
2.3.7 Molecular Electronics	31
2.4 Computational Platforms	31
2.4.1 Application-Specific Integrated Circuits	33
2.4.2 Real-Time Operating Systems	34
2.5 Surveillance, Diagnostics, and Prognostics	35
2.5.1 Model-Based Techniques	37
2.5.2 Data-Driven Techniques	37
2.5.3 Combined Techniques	39
2.5.4 Vision-Based Diagnostics	40
2.6 Control and Decision	40
2.6.1 Continuous Control Methods	42
2.6.2 Discrete Control Methods	47
2.6.3 Combined Continuous and Discrete Control Methods	49
2.6.4 Decision-Making Methods	50

2.7 Human-System Interactions	50
2.7.1 Gaze-Contingent Control and Human-System Interaction with Eye-Tracking Systems	51
2.7.2 Software agent-based Operational Support Systems	52
2.7.3 Virtual Collaborator	53
2.7.4 Content-Based Information Retrieval	54
2.7.5 Biometrics	55
2.7.6 Automated Visual Surveillance for Facility Monitoring.....	55
2.7.7 Virtual Reality.....	56
2.8 High-Integrity Software.....	57
2.8.1 State of the Practice for High-Integrity Software.....	57
2.8.2 Software Development Technologies, Methodologies, and Tools.....	58
2.8.3 Software Assessment Methods and Technologies	59
2.8.4 Object-Oriented Languages: Real-Time Java	61
3. PROSPECTIVE EMERGING TECHNOLOGIES RESEARCH TOPICS	63
3.1 Emerging Technologies Addressed Within NRC Research Plan for Digital Instrumentation and Control.....	63
3.2 Emerging Technologies that Suggest Potential Near-Term Research Needs.....	65
3.3 Emerging Technologies that May Warrant Long-Term Monitoring.....	65
4. REFERENCES	67
APPENDIX.....	A1

EXECUTIVE SUMMARY

This report presents the findings from a survey of emerging technologies in the field of instrumentation and controls (I&C). The report (1) gives an overview of the state-of-the-art in selected technology focus areas for industrial, research, or scientific applications that are relevant to nuclear power plant I&C systems, (2) identifies significant technological advances or projected developments that could impact safety-related applications for upgrades at existing reactors and for near-term or long-term deployment at future nuclear power plants, and (3) suggests potential research needs for consideration and technology trends for monitoring.

The research approach taken for the emerging technology survey was to first identify a set of technological focus areas within the I&C discipline. These technology focus areas are

1. sensors and measurement systems,
2. communications media and networking,
3. microprocessors and other integrated circuits,
4. computational platforms (computers, programmable logic controllers, application specific integrated circuits, etc.),
5. diagnostics and prognostics,
6. control and decision,
7. human-system interactions, and
8. high-integrity software.

The methods employed for the emerging technology survey consisted of literature reviews (in particular, recent scientific and technical journals), Internet searches, vendor contacts, and discussions with technology experts. Input was solicited from nuclear industry representatives, such as plant owners' groups, the Electric Power Research Institute (EPRI), and research teams under the U.S. Department of Energy's (DOE's) Nuclear Energy Research Initiative (NERI) program. In addition, contacts were pursued with other industries such as the steel, chemical, and transportation industries, research institutes such as universities and national laboratories, and other federal agencies, including the U.S. Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA). The findings of this survey are documented in the body of this report.

Based on an assessment of the emerging technology survey findings, observations are drawn about safety-related issues posed by the expected application of state-of-the-art technology for upgrades at existing nuclear power plants and for near-term deployment of advanced reactors. From these observations, this report confirms the timeliness of the research elements in the current NRC Research Plan for Digital Instrumentation and Control, and suggests additional research needs. In addition, some technologies were seen as having potential applications for long-term deployment of future reactor concepts, so they are identified for monitoring and later consideration.

For the sensors and measurement systems technology focus area, several new sensors and sensing techniques are under development as a result of the research stimulus provided by the DOE programs NERI, International NERI, and Nuclear Engineering Education Research (NEER). These new sensors clearly are potential candidates for eventual implementation in nuclear power plants. Most of the sensor technologies described in the report are in a state of research

development or are in the process of demonstrating their capability for nuclear power applications. The new sensors and measurement systems are

1. silicon carbide flux monitor,
2. solid-state neutron flux monitor,
3. fuel mimic power monitor,
4. scintillation-based measurements for temperature and flux,
5. Johnson noise thermometry,
6. ultrasonic flowmeters,
7. magnetic flowmeter for measurement of primary coolant flow,
8. Fabry-Perot fiber optic temperature sensor,
9. optic pressure sensors,
10. gamma ray tomographic spectrometry,
11. hydrogen sensor, and
12. smart sensors.

The NRC Research Plan for Digital Instrumentation and Control contains two research elements that pertain to this technology focus area: §3.5.3 “Advanced Instruments” and §3.5.4 “Smart Transmitters.” The findings of this survey confirm the need for the technology and applications research specified in the research plan. The sensor developments described in this survey serve to identify specific sensor types or characteristics that can be studied or monitored in anticipation of potential use in current, near-term deployment or long-term deployment plants.

The ultrasonic flowmeters have recently come before NRC for review as part of license amendments requesting power rate increases. Thus, the NRC staff has experience with the assessment of this technology through investigation of the accuracy claims of the sensor manufacturers. Continued monitoring of experience with the flowmeters and any further developments is suggested.

Of the emerging sensor technologies still under development, silicon carbide neutron flux monitors, which offer the potential to combine the functions of current three-range flux monitoring into a single system, showed the greatest maturity. Therefore, those instruments are considered to be the most likely new sensor technology for near-term deployment in existing or evolutionary plants, and they are candidates for specific near-term research under the “Advanced Instruments” research activity.

The remaining new sensor technologies for traditional nuclear and process variable measurement (i.e., flux, temperature, flow, pressure) are identified as candidates for long-term monitoring to keep track of their development and anticipate the need for more comprehensive investigations. Two emerging sensor technologies address sensing needs associated with innovative reactor concepts. These are gamma-ray tomographic spectrometry for pellet fuel and core monitoring, and a hydrogen sensor for entrained gas monitoring and facility or process monitoring as part of nuclear-driven hydrogen production. In each case, monitoring the evolution of these technologies is suggested.

Finally, given the potential benefits offered by functional consolidation, self health assessment (e.g., self calibration, heartbeat, onboard diagnostics), and improved information (e.g., signal validation, virtual measurements), it is rightly anticipated that smart sensors will eventually migrate into safety-related applications at nuclear power plants. For those reasons, and because of the market forces that are driving more vendors to intelligent digital product lines, it is observed that this technology should be considered for more thorough investigation in the near term. This

is consistent with the “Smart Transmitter” element of the NRC Research Plan for Digital Instrumentation and Control.

As part of the communications media and networking technology focus area, the survey identified highlights from the technology that represent key advancements or expected developments and significant or evolving approaches. The findings are presented according to an expanding view of network technologies (i.e., from the communications bus structure to the overall network design philosophy). The topics selected are

- high-performance architectures for interconnection platforms,
- communications media (i.e., the physical layer),
- fieldbus (i.e., emerging sensor network protocols),
- security,
- network management, and
- high-level network design approaches.

The NRC Research Plan for Digital Instrumentation and Control contains two research elements that pertain to this technology focus area: §3.5.5 “Wireless Communications” and §3.5.6 “Firewalls.” The findings of this survey confirm the need for the technology and applications research specified in the research plan.

In this survey, it is observed that the use of wireless systems in the nuclear industry is occurring now and is expected to significantly increase in the near term because of their cost, availability, and flexibility. Given the limited experience with wireless communications for highly reliable, secure data communications, near-term research is needed to better characterize the deployment issues (e.g., reliability, security, and electromagnetic compatibility) that should be addressed to enable safety-related applications of this technology. Based on the rapid pace of advancement and product development for this emerging technology, the recently initiated research project is timely.

Firewalls are key considerations in addressing network security. However, there are many other aspects related to both external and internal security. While the survey identifies prominent security techniques, a thorough investigation of the subject has merit. In light of increased security awareness and the introduction of wireless communications into process control systems, recent research by NRC into the network and computing security is well justified and should proceed by addressing the full range of techniques.

Of the other topics, sensor networks or fieldbus technologies are identified as candidates for near-term research. Implementation of wireless transmitters is beginning in nonsafety applications at nuclear power plants. It is expected that networks for field devices will be the norm for control and information systems in new plants. The technological evolution of the sensor market and desires to reduce cabling costs are expected to give momentum to the expanded use of sensor networks (both wired and wireless) in the nuclear power industry. As a result, it seems clear that near-term research into the safety characteristics of fieldbus technologies is warranted and should be considered as a part of the NRC Research Plan on Digital Instrumentation and Control.

High-performance architectures and new developments in the more conventional communications media (i.e., wired and optical) are identified as emerging technologies that have the potential for eventual migration into safety-related nuclear power applications. Architectural developments have the potential to impact the distributed computing and high-speed data processing capabilities

that are likely to be prominent in the integrated, autonomous control and information systems at future nuclear power plants. Therefore, these developments should be monitored and, as capabilities mature, investigated more thoroughly in terms of performance and reliability characteristics. NRC has experience evaluating plant communications systems based on wired and optical communications media; however, projected development in each area will probably significantly increase the available bandwidth for data systems while raising reliability and environmental compatibility issues. Therefore, it seems reasonable to monitor the state of the technology for these communications media.

Finally, trends in fundamental techniques or approaches may affect the implementation and use of networks in future nuclear power plants, so it is suggested that NRC maintain technical familiarity with the state-of-the-art in those areas. Specifically, the trend toward highly interconnected distributed computing systems for autonomous control of complex process systems suggests that the capabilities of network management solutions probably will have to be considered in the assessment of safety-related control and information systems for future nuclear plants. Also, evaluation of emerging network design approaches may become an important consideration in the review of future plants with highly interconnected, distributed computing environments for autonomous control and information systems.

In the microprocessors and other integrated circuits (ICs) technology focus area, the survey identified highlights from the technology that represent key advancements or expected developments and significant or evolving approaches. Several IC technologies are identified as meriting long-term monitoring because of their significance for nuclear application or their innovation in the field. These technologies are

- radiation-hardened ICs,
- system of a chip (SoC) circuitry,
- optical processors (in particular, optical digital signal processors),
- vertically-stacked ICs,
- nanotriodes, and
- microelectromechanical systems (MEMS).

Molecular electronics are also identified as an emerging technology, but the survey concluded that molecular electronics do not offer even long-term likelihood for nuclear power application.

The potential impact toward facilitating smart sensors and sensor networks in containment applications in the long term suggests the value of maintaining awareness of developments for rad-hard ICs. Likewise, the potential for sensing applications using SoC circuitry that can be located in harsh environments at future reactors and then changed out (perhaps robotically) on a periodic basis provides motivation for monitoring the long-term trends in SoC development.

As noted in this report, NRC has experience evaluating optical interconnections that have been implemented in nuclear plants as part of fiber-optic communications links. Although, safety-related application of optical processing seems unlikely in the near term, the potential increase in computational speed promised by optical digital signal processors (ODSPs) suggests that usage over the long term is likely. Therefore, awareness of this technology should be maintained.

Three unique chip fabrication processes are identified as meriting long-term monitoring. Vertically-stacked ICs can lead to a dramatic improvement in circuit density. Nanotriodes can make possible an environmentally (especially rad-hard) robust alternative to field effect

transistors. MEMS technology can lead to the prospects of unique, versatile sensors. The potential for impacting safety-related nuclear power applications as a result of these developments could include previously unavailable measurements that give new insight into the plant status. Additional positive impacts of new technologies are the migration of smart sensors into the most inhospitable areas within the reactor containment or the use of new computational power and speed to support more extensive model-based surveillance and diagnostics systems that are capable of detecting incipient failure.

In the computational platform technology focus area, two key technologies are identified. These are application-specific integrated circuits (ASICs) and real-time operating systems. There have been a limited number of specialized ASIC-based applications developed specifically for the nuclear industry. In light of the potential costs for dedicated commercial software-based systems, it is possible that development of ASIC-based components for nuclear power safety applications will expand in the long term. Therefore, maintaining an awareness of the emerging technology of ASICs is warranted. Because operating systems provide the fundamental interface between software and hardware in most digital applications, their performance and reliability characteristics should be well understood. The NRC Research Plan for Digital Instrumentation and Control contains a research element (§3.2.6 “Operating Systems”) that addresses the research need in this area. Therefore, the survey findings are consistent with the research plan. As an additional observation, participation by the NRC in software standards activities would prove beneficial for advocating safety considerations in real-time operating systems.

The surveillance, diagnostics, and prognostics technology focus area is characterized by a plethora of existing and developing techniques. Many examples of surveillance and diagnostics techniques have been applied to nuclear power process and equipment monitoring over the years. However, recent activity under the NERI and NEER programs has stimulated development of new applications focused on nuclear power. Examples are given in the report. For this survey, four categories are identified. Those are

- model-based techniques,
- data-driven techniques,
- combined techniques (i.e., model-based and data-driven), and
- vision-based techniques.

The NRC Research Plan for Digital Instrumentation and Control contains a research element (§3.5.2 “Predictive Maintenance/On-Line Monitoring”) that addresses surveillance, diagnostics, and prognostics. Because of the likely integration of control and diagnostics for autonomous plant operation and the expected greater reliance on surveillance and prognostic methods to facilitate predictive maintenance, the survey findings confirm the need for such research. Several developing techniques are being targeted for nuclear power applications so it would seem reasonable to conduct research in the near-term on the capabilities that those techniques provide. In particular, methods for assessing the accuracy, stability, and reliability of diagnostic and prognostic techniques are appropriate candidates for near-term research. In addition, it is reasonable to monitor development in the technology through awareness of applications in other industries.

In the control and decision technology focus area, numerous control and decision techniques or approaches were surveyed. These methods include

- linear matrix optimal control,
- nonlinear control,
- intelligent control (fuzzy control and neural network control),
- adaptive control,
- genetic algorithm-based control,
- multimode control,
- hierarchical supervisory control,
- expert system control (stated-based or data-based),
- intelligent agent-based control,
- multilevel flow model control,
- formal methods control,
- object-oriented control,
- hybrid control, and
- decision-making methods (model-based, rule-based, data-driven, or knowledge-based)

NRC has significant experience reviewing control systems based on classical control techniques. Much less (or, in some cases, no) experience exists with the so-called “advanced” control techniques. However, it does not seem necessary or cost effective for each and every method to be researched to assess its performance and reliability characteristics. Instead, it seems sufficient for a general knowledge to be maintained by following long-term developments in the investigation and application of control and decision techniques (primarily by universities and national laboratories or in other industries such as fossil power).

The most significant change that is expected in control system development for nuclear power may be the transfer of more and more of the decision-making responsibility to I&C systems. Given the staffing and operational cycle goals of long-term deployment reactor concepts and the prospect of multi-modular plants with integrated process systems and/or control rooms, the move to highly automated control and information systems seems inevitable. Consideration should continue to be given to the role of the human in nuclear plant operations (which cross cuts the human factors engineering and controls disciplines) and the capabilities and reliability of autonomous control systems. In particular, familiarity with the capabilities and configuration options of highly autonomous control systems, which will integrate control, diagnostic and decision-making functions, should be developed before the long-term deployment concepts reach fruition.

In the technology focus area of human-system interactions (HSI), selected emerging technology highlights involving interaction approaches for operator support, information retrieval, control room design and assessment, biometrics and site security, and virtual reality are identified. Although HSI is not explicitly part of the NRC Research Plan for Digital Instrumentation and Control, it is observed that several interaction technologies warrant long-term monitoring and may pose research needs that can be addressed in conjunction with human factors engineering research. In particular, the expected assumption of greater decision-making responsibility by autonomous, intelligent control and information systems gives rise to a research challenge for the designer, suppliers, owners, and regulators. Participation in existing international research is reasonable, and interaction with industry groups (DOE, EPRI, owners’ groups) in identifying and studying the issues posed by this trend is warranted.

In the survey of high-integrity software, the state-of-the-practice in software engineering is described, highlights of emerging trends in software development and assessment are given, and a description of an emerging real-time software language that may see increased use is provided.

High-integrity software is addressed in the NRC Research Plan for Digital Instrumentation and Control (§3.3 “Software Quality Assurance”). Two key topics in that field are specifically addressed—software development (§3.3.1 “Investigate Objective Software Engineering Criteria”) and software assessment (§3.3.2 “Investigate Criteria for Software Testing”). The findings of the survey confirm the significance of these research topics and the need for near-term attention. Two observations for particular research subjects are that methods for development of high-integrity software using more formal software engineering methods (such as the Cleanroom approach) should be investigated and that developments in the statistics of rare events for testing and assessment of very high integrity systems should be followed.

The findings, observations, and conclusions from this survey serve as input for the on-going process of refining and enhancing the NRC Research Plan for Digital Instrumentation and Control. The emerging technologies that are identified in areas that correspond to research elements already addressed in the I&C research plan confirm its technical focus and suggest specific topics that may contribute to establishing the detailed research approach to be followed. The near-term research needs for emerging technologies that are identified in areas not directly addressed in the I&C research plan offer supplementary topics that can be considered in subsequent enhancement of the plan. The emerging technologies identified as warranting long-term monitoring provide pointers to technologies that are generally not considered to be sufficiently mature or well demonstrated to impact near-term deployment but which may lead to potential future research needs. Finally, it should be noted that this survey proves a “broad-brush” overview of a significant number of technical topics. It is recommended that periodic surveys be conducted of specific technology focus areas (or subsets thereof) to provide more depth in the identification and assessment of emerging technologies with the potential to impact safety-related I&C applications in nuclear power.

ACROYNOMS

3D	three dimensional
ABWR	advanced boiling-water reactor
AIS	adaptive intelligent system
ALMR	advanced liquid-metal reactor
AlN	aluminum nitride
ALWR	advanced light-water reactor
ANFIS	adaptive network-based fuzzy inference system
ANN	artificial neural network
ANP	Advanced Nuclear Power
ANSI	American National Standards Institute
APACS	advanced plant analysis and control system
ASIC	application-specific integrated circuit
ATM	asynchronous transfer mode
AVS	automated visual surveillance
B&W	Babcock and Wilcox
BBIC	bioluminescent bioreporter integrated circuit
BIA	Berufsgenossenschaftliches Institut für Arbeitssicherheit
BIOS	basic input output system
CAN	controller area network
CCD	charge-coupled device
CDMA	code division multiple access
CeBASE	Center for Empirically Based Software Engineering
CFR	causal functional representation
CMM	Capability Maturity Model
CMOS	complementary metal-oxide semiconductor
COTS	commercial off-the-shelf
CPU	central processing unit
CZT	cadmium zinc telluride
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DVD	digital versatile disc
DSP	digital signal processor
EAL	evaluation assurance levels
EDGE	enhanced data rate for global evolution
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EO	electro-optical
EPRI	Electric Power Research Institute
FDI	fault detection and isolation
FIR	finite impulse response
FPGA	field programmable gate array
FTS	flexible tooling system
GaAs	gallium arsenide
GAN	Gosatomnadzor
Gbps	gigabits per second
GC	garbage collector

GCR	galactic cosmic rays
GMDH	group method of data handling
GVSC	generic VHSIC space-borne computer
GSM	global standard for mobile communications
HAL	hardware abstraction layer
HRP	Halden Reactor Project
HSI	human-system interaction
HTGR	high-temperature, gas-cooled reactor
I&C	instrumentation and controls
I/O	input/output
IC	integrated circuit
ICMP	Instrumentation Calibration Monitoring Program
ICS	integrated control system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INERI	International Nuclear Energy Research Initiative
InP	indium phosphide
IP	internet protocol
ISO	International Organization for Standardization
KAERI	Korea Atomic Energy Research Institute
kbps	kilobits per second
LAN	local area network
LQG	linear quadratic gaussian
LTR	loop transfer recovery
MBC	model-based control
Mbps	megabits per second
MCC	motor control center
MEMS	microelectromechanical systems
MFM	multilevel flow model
MIPS	million instructions per second
MMIS	man-machine interface systems
MOS	metal-oxide semiconductor
NASA	National Aeronautics and Space Administration
NEER	Nuclear Engineering Education Research
NEPO	Nuclear Energy Plant Optimization
NERI	Nuclear Energy Research Initiative
NIC	network interface card
NIST	National Institute of Standards and Technology
NLO	nonlinear optical
NMOS	nonvolatile metal-oxide semiconductor
NR	narrow range
NRC	U.S. Nuclear Regulatory Commission
OASIC	optical application-specific integrated circuit
OASIS	optimal aircraft sequencing using intelligent scheduling
ODSP	optical digital signal processor
ODSPE	optical digital signal processing engine
ORNL	Oak Ridge National Laboratory
PBMR	pebble bed modular reactor
PC	personal computer
PCA	principal component analysis
PCB	printed circuit board

PCI	peripheral component interconnect
PCS	plant control system
PDA	personal digital assistant
PID	proportional-integral-derivative
PKI	public key infrastructure
PLC	programmable logic controller
PNNL	Pacific Northwest National Laboratory
POSIX	portable operating system interface
PSP	Personal Software Process
PWR	pressurized-water reactor
rad-hard	radiation-hardened
RETSINA	reusable environment for task-structured intelligent networked agents
RF	radio frequency
RFC	request for comment
RFI	radio frequency interference
RFID	radio frequency interference identification
RPS	reliability prediction systems
RTSJ	real-time specification for Java
SAN	storage area network
SDMS	self-diagnostic monitoring system
SEE	single-event effects
SEI	Software Engineering Institute
SEL	Software Engineering Laboratory
SISO	single input, single output
SNMP	simple network management protocol
SoC	system on a chip
SSFm	solid-state flux monitor
TDM	time-domain multiplexing
TDMA	time division multiple access
TSP	Team Software Process
UTSG	U-tube steam generator
UWB	ultrawideband
VDU	video display unit
VHSIC	very-high-speed integrated circuit
VPN	virtual private network
VR	virtual reality
WARES	Warwick Automation Research and Evaluation System
W-CDMA	wideband code division multiple access
WDM	wavelength-division multiplexing
XML	eXtensible markup language
XRN	eXpandable resilient networking

1. INTRODUCTION

This report presents the findings from a survey of emerging technologies in the field of instrumentation and controls (I&C). The report (1) gives an overview of the state-of-the-art in selected technology focus areas for industrial, research, or scientific applications that are relevant to nuclear power plant I&C systems, (2) identifies significant technological advances or projected developments that could impact safety-related applications for upgrades at existing reactors and for near-term or long-term deployment at future nuclear power plants, and (3) suggests potential research needs for consideration and technology trends for monitoring.

1.1 Objectives of the Emerging Technology Survey

The purpose of this report is to document a survey of the state-of-the-art for a wide range of technology areas within the I&C discipline. This effort is part of an ongoing activity expected to provide periodic reports on the status of specific technologies that have potential applicability for safety-related systems in nuclear power plants and pose emerging research needs. This initial survey consists of a broad-brush overview of I&C technologies and serves as a baseline for the series of periodic reports specified in the U.S. Nuclear Regulatory Commission (NRC) Research Plan for Digital Instrumentation and Control (SECY-01-0155). More than just a list of technologies, the survey also provides high-level discussions of specific emerging capabilities and equipment in each technology area that has potential for safety-related applications at nuclear power plants—either through upgrades at existing plants or as design elements of advanced reactor concepts. From the survey findings, suggestions of prospective research needs are developed.

1.2 Research Approach for the Emerging Technology Survey

The research approach taken for the emerging technology survey was to first identify a set of technological focus areas within the I&C discipline. Then, based on these focus areas, the multidisciplinary expertise at Oak Ridge National Laboratory (ORNL) was employed to generate a baseline for identification of technology advances and characterization of the state-of-the-art. From the beginning, the I&C research team at NRC was consulted for confirmation of current research priorities and expectation of future research needs. In addition, an I&C consultant from the nuclear power industry was engaged as a participant and co-author to provide an insider's perspective on expectations for I&C technology over the next decade.

As the next step in the survey, investigations were conducted that consisted of literature reviews (in particular, recent scientific and technical journals), Internet searches, vendor contacts, and discussions with technology experts. Input was solicited from nuclear industry representatives, such as plant owners' groups, the Electric Power Research Institute (EPRI), and research teams under the U.S. Department of Energy's (DOE's) Nuclear Energy Research Initiative (NERI) program. In addition, contacts were pursued with other industries such as the steel, chemical, and transportation industries, research institutes such as universities and national laboratories, and other federal agencies, including the U.S. Department of Defense (DoD) and National Aeronautics and Space Administration (NASA). The findings of this survey are documented in the body of this report.

Finally, on the basis of the combined expertise from the ORNL staff, NRC research staff, and industry consultant, observations are drawn about safety-related issues posed by the expected application of state-of-the-art technology for upgrades at existing nuclear power plants and for near-term deployment of advanced reactors. From these observations, this report confirms the timeliness of the research elements in the current NRC Research Plan for Digital Instrumentation and Control and suggests additional research needs. In addition, some technologies were found to

present the potential for eventual nuclear plant applications as part of the long-term deployment of future reactor concepts, so they are identified for monitoring and later consideration.

1.3 Scope of the Emerging Technology Survey

The field of I&C technologies is broad and varied. It can be visualized in two slices. The “vertical” slice, which is functionally focused, addresses the technologies that embody the sensing, communications, monitoring, control, and presentation and command systems between the process (i.e., the reactor, heat transport, and energy conversion systems) and the plant personnel (i.e., operations and maintenance staff). The “horizontal” slice at the lowest level is equipment focused and consists of the instrumentation string from the sensors and signal processing elements to the diagnostic modules and controllers (e.g., computational platforms) to the actuation devices. The variety of technologies that constitute the I&C systems of a nuclear power plant can be difficult to address as a whole. Therefore, the tack taken in this survey is to identify technology focus areas.

Based on the “horizontal” or equipment-focused slice, the I&C technology breakdown is as follows:

- sensors,
- communications media,
- microprocessors and other integrated circuits, and
- computational platforms (computers, programmable logic controllers, application-specific integrated circuits, etc.).

Actuation devices, such as pumps, valves, control rod drive mechanisms, and the like, are not included as a technology focus area for this survey. This position is taken to limit the scope of the survey to a manageable level by excluding process equipment that is typically addressed in other disciplines. Thus, unique actuation devices needed for innovative reactor concepts (e.g., pebbled fuel, hydrogen production, volatile or corrosive coolants) are also not described in this report. The technologies involved with the electronics that command the traditional actuation devices for light-water reactors are currently well understood. Any new technologies for digital implementations are considered part of the plant controllers and are thus addressed under the microprocessor and computational platform categories. Concerning microprocessors, the current trend for general-purpose central processing units (CPUs) is directed toward higher circuit density and faster processing speeds. However, little value would be added to this investigation by listing the latest and fastest microprocessors as part of this survey because the technology is evolutionary rather than revolutionary, and the pace of product introduction in the computing industry results in rapid obsolescence of specific microprocessors. Thus, the report focuses on significant changes in the base technology for this focus area. The state-of-the-art for computational platforms lies in the field of supercomputing, but that is of little relevance to nuclear power or process industries. Therefore, the survey in this technology focus area is limited to selected highlights regarding platforms and system software that are targeted for business and industrial application.

Based on the “vertical” or function-focused slice, the I&C technology breakdown is as follows:

- measurement systems,
- communications or networking,
- diagnostics and prognostics,
- control and decision,

- human-system interaction, and
- high-integrity software.

For the purposes of this survey, the discussion of human-system interaction technology is brief and limited to selected evolving capabilities or tools. Because of the frequent characterization of human factors engineering as a specialized discipline within the I&C field, it would be difficult to give comprehensive coverage of that technology focus area. Thus, only a limited number of highlights are given, which represent concepts or systems that are being incorporated in or may migrate into nuclear power applications over time.

Therefore, the chosen list of technology focus areas is derived from the technology breakdown that offered by each of the two slices. The topics covered in this report are

1. sensors and measurement systems,
2. communications media and networking,
3. microprocessors and other integrated circuits,
4. computational platforms,
5. diagnostics and prognostics,
6. control and decision,
7. human-system interactions, and
8. high-integrity software.

As a practical matter, given limitations in resources as well as the breadth of the subject matter, this survey cannot be exhaustive. Thus, the emphasis followed while conducting the review and presenting the findings is the identification of prominent I&C technologies that are in general application or are under development within commercial industries, research organizations, and governmental agencies (e.g., NASA, DoD). Thus, for the selected technology focus areas, the report attempts to highlight key advances or expected developments that may have an impact on nuclear plant I&C or may eventually migrate into nuclear power applications. Based on these observations, conclusions are drawn about likely technology issues and research needs over the coming decades that should be considered in the continuing refinement of the NRC Research Plan for Digital Instrumentation and Control. Technology issues considered in this survey concern either (1) near-term issues arising from upgrades at existing reactors and deployment of evolutionary reactor designs or (2) long-term issues projected for deployment of innovative reactor concepts (i.e., Generation IV plants). As a final note on the scope of the findings, the broad nature of this survey precludes specific research recommendations, so the observations and conclusions provided represent suggested topics for either further investigation in the near term or identification of technology trends that should be monitored over the long term.

1.4 Structure of the Emerging Technology Report

The information presented in this report consists of the findings from the emerging technology survey and observations regarding specific state-of-the-art capabilities, techniques, and components that are candidates for near-term deployment of nuclear applications in existing and evolutionary reactors or may eventually be candidates for deployment in long-term advanced reactor concepts.

Section 2 documents the state-of-the-art and expected developments that were identified for each technology focus area within the broad field of I&C technologies. The eight sections that correspond to each specific technology focus area begin with a brief description of the status for the subject technology in the nuclear power industry. Next, the primary findings of the emerging

technology survey are presented as overviews of the advanced capabilities, techniques, and/or components that represent the state-of-the-art in that focus area. These discussions include some examples of the application base of the focus technology within other industries and organizations and indicate foreseeable applicability as part of near-term or long-term deployment for nuclear power.

Section 3 presents observations and conclusions about emerging technologies identified in the survey that pose potential safety-related issues. These safety issues are described in terms of those that are identified in the NRC Research Plan for Digital Instrumentation and Control, those that should be considered for near-term research and those that should be monitored because future development may increase their potential for migration into safety-related nuclear applications.

2. STATE-OF-THE-ART DEVELOPMENT FOR I&C TECHNOLOGIES

2.1 Sensors and Measurement Systems

Sensors and measurement systems are the fundamental means of extracting information about the dynamic state of nuclear reactors and the associated energy conversion systems (i.e., the nuclear steam supply system and balance-of-plant systems) to enable monitoring, controlling, and regulating nuclear power plants. Given the range of sensing techniques in existence within the various process industries (such as chemical, pharmaceutical, petrochemical, steel, pulp and paper), the survey in this technology focus area is primarily limited to those measurement systems that relate to the traditional measured variables within the nuclear power industry. The term measurement system is included in the technology designation because a measurement function may be accomplished by single sensing element/transmitter components, more complex combinations of sensors, or sensors with embedded intelligence.

The measurement systems, comprised of the sensing element, transducer, and signal-conditioning electronics, in currently operating nuclear power plants have not changed appreciably since their original design and are primarily based on conventional instruments and methods. The principal variables measured for safety-related applications continue to be neutron flux, temperature, pressure, flow, position, and level. The *Nuclear Power Reactor Instrumentation Systems Handbook*,¹ published in 1973 by the U.S. Atomic Energy Commission, still provides a good general picture of the sensing systems employed in currently operating nuclear power plants.

Some new sensor types are being employed as upgrades in current nuclear power plants; in particular, the ultrasonic flowmeters are being used in balance-of-plant systems. In addition, research has been initiated in recent years to develop innovative sensor technologies to measure traditional nuclear power plant variables. These emerging sensor technologies are the primary subject of the survey in this focus area. Some information is also included about selected sensors for nontraditional variables that may see application in nontraditional reactor concepts (i.e., non-light-water reactors). Also, some approaches for advanced measurement systems are noted as developing trends. Finally, radically different sensing systems such as on-line fuel condition monitoring to allow operation until just before failure or on-line fuel xenon monitoring have not yet entered the research stage, so they are not specifically addressed in this survey.

2.1.1 Silicon Carbide Flux Monitor

Silicon carbide neutron flux monitors offer the potential to combine the functions of current three-range flux monitoring into a single system and further offer the potential to eliminate the added complexity of a separate gamma compensation system. Silicon-carbide-based flux monitors² depend upon the production of a few-micron-thick, charge-depleted silicon carbon layer on top of a silicon carbide substrate—generally a Schottky barrier type device. A layer of ⁶LiF is deposited across the top of the device to convert incident neutrons into charged particles. The top and bottom of the layer are electrically connected to a standard charge-sensitive amplifier and a nuclear pulse spectroscopy circuit.

The chief advantages of this emerging sensor technology are that silicon carbide shows considerable radiation hardness [with reported functioning to fast neutron fluences up to 10^{17} n/cm² ($E_n > 1$ MeV)]. It offers high-temperature tolerance (potentially up to 800°C) while permitting high-speed operation (potentially gigahertz), and it provides the inherent ability of small active-volume devices to discriminate against gamma dose in pulse-mode operation. Both the relatively high burn-up rate of the ⁶Li and the overall radiation tolerance will likely restrict the devices to ex-core use. Nevertheless, this type of device shows high promise as an ex-core

neutron flux monitor and will likely see eventual widespread use as the technology matures. An understanding of the characteristics and capabilities of such devices may prove necessary in the near term, depending on the continued development of the technology.

2.1.2 Solid-State Neutron Flux Monitor

A solid-state flux monitor is currently under development as part of an International Nuclear Energy Research Initiative (INERI) project jointly sponsored by DOE and Korean Ministry of Science and Technology. This flux monitor is based on the flux-induced change in electrical resistance of a Group III nitride solid. Because the detector is a solid, no gas seals are required as for conventional technologies. The detector is also expected to be mechanically robust, highly temperature tolerant, and inexpensive.

As currently conceived (see Fig. 2.1), the in-core version of the solid-state flux monitor (SSFM) is based on a polycrystalline AlN compact with evaporated metal contacts. The detector functions by intercepting a small fraction of incident neutrons in the $^{14}\text{N}(n,p)^{14}\text{C}$ reaction. The Group III nitrides are very chemically stable, are mechanically rugged, have wide band gaps, and have high electrical carrier mobilities. The electrical conductivity of AlN at temperatures of 300 K is typically over 10^{14} $\Omega\text{-cm}$. Even at 1300 K, AlN remains a very good insulator with less than a one part per million temperature-induced error expected in a power-range flux measurement. The reaction imparts a net kinetic energy to the energetic daughters of 627 keV. As the energetic daughters slow down in the nitride matrix, they excite electrons into the conduction band. The excited electrons are free to move under an applied bias, resulting in a neutron-flux induced electrical current. The detector is intended to be operated in current mode, and it will also be sensitive to gamma rays. Thus, the SSFM will be limited to operation in reactor power-range fluxes. The main limitation to this detector is its embryonic state of development. Because of the potential performance benefits of these devices for in-core flux mapping, the progress in demonstrating this technology should be monitored over the long term.

2.1.3 Fuel Mimic Power Monitor

The fuel mimic power monitor has been developed and demonstrated through Nuclear Engineering Education Research (NEER) program and EPRI funding. The instrument represents a unique sensing technology in that it provides a direct measurement of the nuclear energy deposited into a fuel mimic mass.³ The fuel mimic power monitor is based on the addition of heat through resistive dissipation of input electrical energy to a small mass of reactor fuel or fuel analogue. A feedback loop controls the input electrical energy needed to maintain the fuel mass at a nearly constant temperature regardless of the nuclear energy deposited in the mass. Energy addition to the fuel and fuel temperature feedback to the controller are provided by a resistive heating element embedded in the fuel mass. As long as the external heat transfer environment remains constant, the input electrical energy is inversely related to the actual nuclear energy deposition. The main advantage of this type of sensor is that it provides a close analog to the actual physical process of interest (cladding temperature). The major concerns about the technology relate to its sensitivity to its heat transfer environment. If the electrical energy is not deposited spatially in the same manner as the nuclear energy is generated, the consequent heat distribution difference will produce an erroneous reading. The device also relies on an accurate temperature measurement. The progress in continued research on this technology should be monitored over the long term because the potential introduction of this unique measurement capability could impact operating margins.

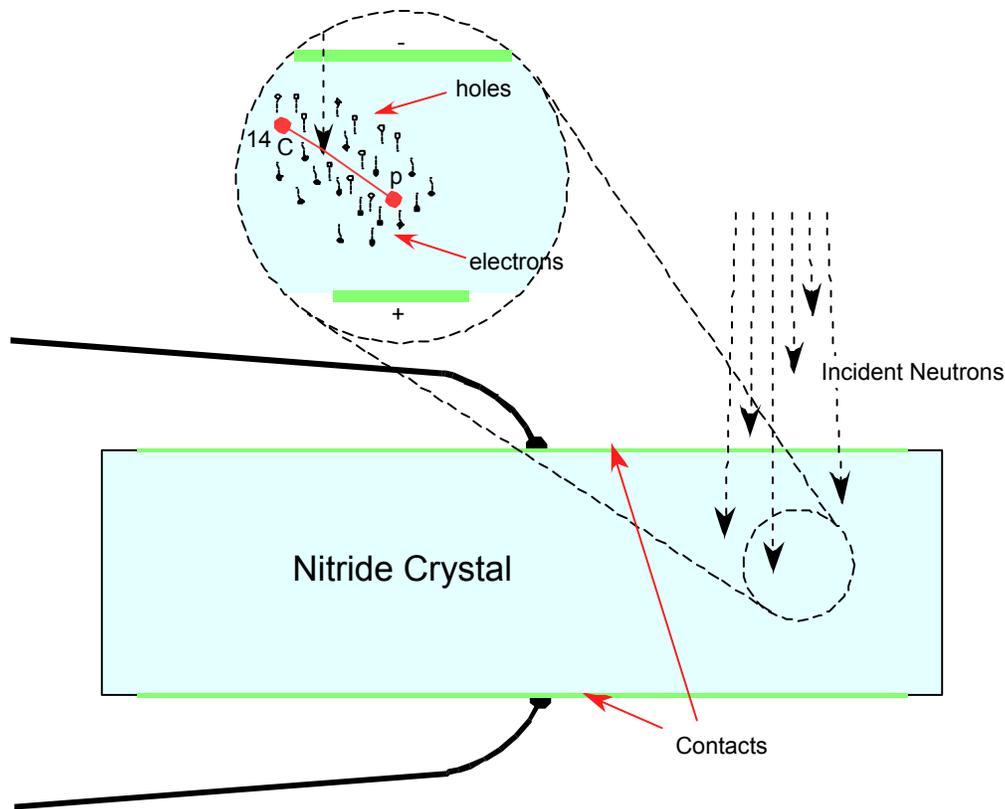


Figure 2.1. General concept of solid-state flux monitor.

2.1.4 Scintillation-Based Measurements

A miniature scintillation-based, in-core, self-powered neutron flux and temperature probe is currently under development as part of a NERI project. Because of extreme environmental challenges, detailed in-core process knowledge (e.g., flux and temperature) has always been limited. This emerging sensor technology is directed at obtaining more accurate, reliable, cost-effective determination of in-core power density to facilitate higher fuel burn-up, more efficient core loadings, and uniform power distributions. Although the probe would be generally applicable to any reactor technology, it is being specifically targeted to accommodate the higher core temperatures of high-temperature, gas-cooled reactors (HTGRs).

Scintillation-based measurements have the potential to function effectively in or near an HTGR core. The primary deficiency in the technology preventing its use for in-core measurements has been the lack of an effective technique for measuring light within reactor core environments and the rapid darkening of fiber optic light pipes in high radiation fields. Additionally, scintillation materials darken too rapidly to be useful in bulk form near a nuclear reactor core. The current research is attempting to address these concerns. In the detector concept being developed under the NERI project (see Fig. 2.2), a thin film of scintillator is placed at the distal end of a hollow silica tube. The tube is lined with a mirror coating of platinum. The platinum-coated silica tube serves as a hollow-core light guide. The interior of the hollow tube is filled with a noble gas at reactor pressure. The scintillator material is deposited as a few-micron-thick film to allow separation of gamma- and neutron-induced pulses due to the characteristic path differences of their respective induced energetic charged particles (similar to the silicon carbide detector described above). Moreover, the required optical path length of the scintillation photons becomes very small because of the thin layer of scintillator, so radiation darkening is not expected to be a

problem. The major limitation to this technique is its early level of development. Again, because of the potential impact on core performance and operating margins, the development of these devices should be monitored over the long term.

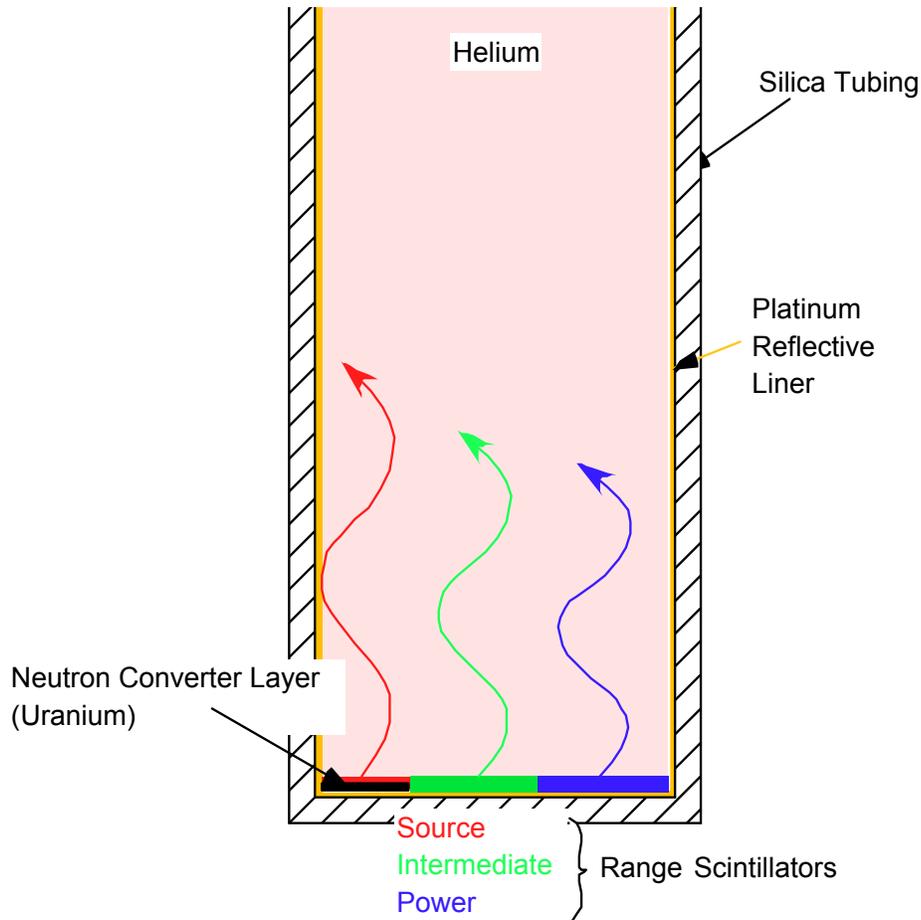


Figure 2.2. Scintillation flux/temperature detector conceptual layout.

2.1.5 Johnson Noise Thermometry

A team of U.S. and Korean researchers are in the process of developing and demonstrating a Johnson noise thermometer for primary flow-loop temperature measurement. Temperature measurements derived from Johnson noise are inherently drift free. Moreover, Johnson noise is insensitive to the material condition of the sensor and, consequently, is immune to the contamination and thermo-mechanical response shifts that plague thermocouples and resistance thermometers. Commercialization of Johnson noise thermometers has the potential to increase the accuracy of primary-loop temperatures with the added benefit of reduced calibration requirements.

Johnson noise is a fundamental representation of temperature—it results from the vibration of the electronic field surrounding atoms as they thermally vibrate. Since temperature is merely a convenient representation of the mean kinetic energy of an atomic ensemble, measurement of these electronic vibrations yields the absolute temperature of the observed fluid. Johnson noise thermometry has been under development for nuclear applications for almost 30 years under DOE and NASA sponsorship. Of special interest, the Japan Atomic Energy Research Institute⁴

recently published a favorable analysis of the potential application of Johnson noise thermometry to in-core temperature measurement. However, limitations regarding its sensitivity to electromagnetic noise and the complexity of the implementation (leading to the need for skilled operators) have hindered widespread industrial acceptance of the Johnson noise measurement technique. It is because of recent advances in digital signal processing that the NERI research team expects to significantly improve the ability of Johnson noise thermometry to withstand electromagnetic noise. Although this development is just beginning, the progress of the digital implementation of this technology should be monitored over the long term considering the value of drift-free, fundamental measurement of primary coolant temperature.

2.1.6 Ultrasonic Flowmeters

There are two distinct types of ultrasonic flowmeters currently being marketed to nuclear power plants: cross-correlation flowmeters and transit-time flowmeters. Both sensor types offer significant reduction in measurement uncertainty.⁵ These instruments are included in this report because they represent an example of an emerging technology that has moved into nuclear applications and has prompted licensing amendments (i.e., power rate increases). Thus, the NRC staff has experience with the assessment of this technology through investigation of the accuracy claims of the sensor manufacturers. Continued monitoring of experience with the flowmeters and further developments is suggested.

Cross-correlation flowmeters emit ultrasonic pulses across a pipe perpendicular to the flow direction at two different locations along the pipe. This flowmeter uses the time delay for pulse reception at each station to determine the flow rate. Cross-correlation flowmeters consist of two sets of externally mounted transducers. Transit-time flowmeters⁶ measure the time-of-flight for the acoustic energy from ultrasonic pulses emitted between two transducers immersed in the fluid. The transit-time flowmeters determine the flow rate based on the differences in transit times upstream and downstream. A multichord implementation of the transit-time flowmeter uses many different acoustic paths across the pipe to map the fluid velocity as a function of position within the pipe. This can reduce sensitivity to the flow profile. These flowmeters consist of multiple sets of in-line transducers.

2.1.7 Magnetic Flowmeter for Measurement of Primary Coolant Flow

Advanced magnetic excitation schemes and signal processing algorithms have been developed over the past decade to reduce the drift to zero, increase the response speed, and reduce the noise sensitivity of commercial magnetic flowmeters. Emerson process controls has been sponsoring research with Purdue University's Nuclear Engineering Department to develop an intelligent signal transmitter incorporating modern methodologies.⁷ Under the U.S.-Korea INERI program, demonstration of a magnetic flowmeter suitable for primary flow measurement in pressurized-water reactors (PWRs) is under way. The capability to directly measure primary flow rather than rely on inferential determination of flow based on primary coolant pump speed could impact operational margins. Magnetic flowmeters are highly accurate ($\pm 1/4\%$ under ideal conditions), respond linearly, and are obstructionless (no fouling, no pumping power consumption). Magnetic flowmeters can also be designed to have minimal sensitivity to a flow profile. In addition, the transmitter for magnetic flowmeters can be located remotely (up to tens of meters away) from the point of measurement, thus reducing environmental exposure.

Magnetic flowmeters operate on the principle that whenever a conductor (in this case, the primary coolant) is passed through a magnetic field, a voltage is generated which is proportional to the velocity of the conductor. Physically, a magnetic flowmeter consists of signal processing apparatus (the transmitter), magnetic coils, and electrodes (to measure the potential across the

coolant) (see Fig. 2.3). The magnetic coils and electrodes are typically implemented as part of a short segment of pipe made of nonmagnetic material that has a nonconductive inner surface containing or pierced by electrodes. Non-wetted, capacitively coupled models are available to allow operation with very low conductivity fluids such as pure water.

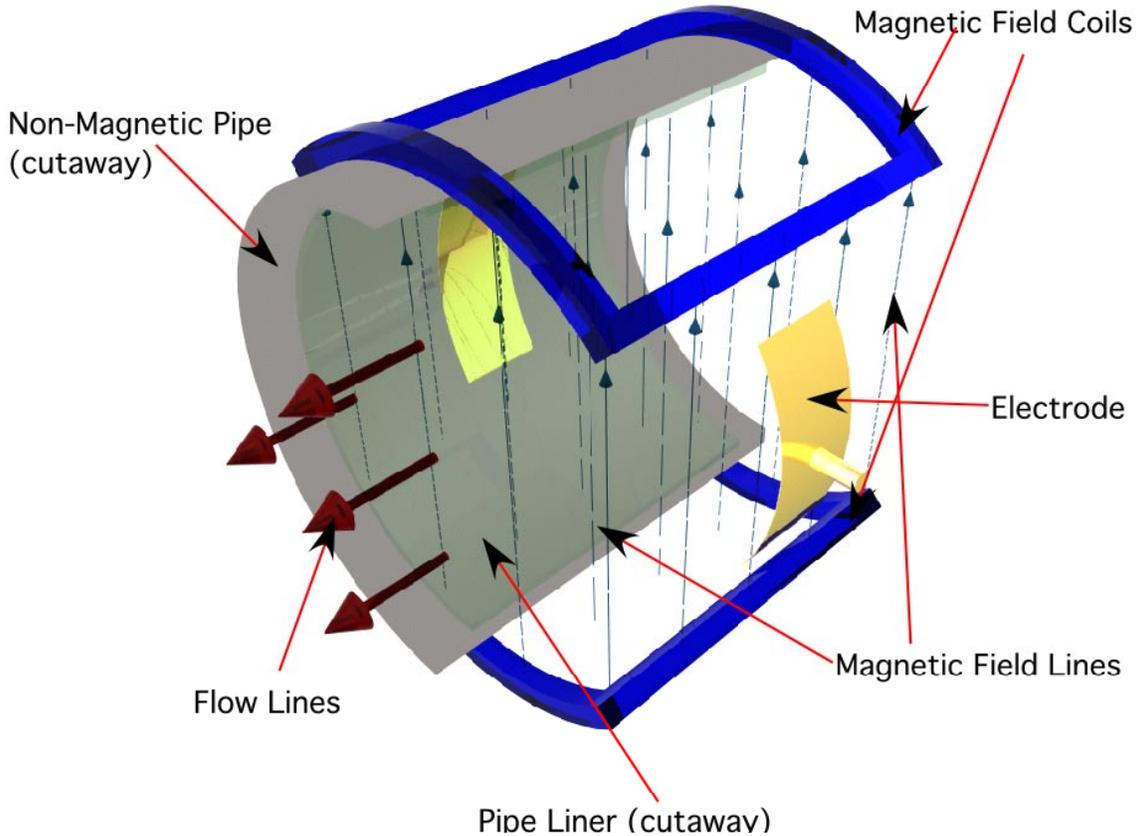


Figure 2.3. Cutaway view of magnetic flowmeter with non-wetted, capacitively coupled electrodes.

To date, radiation sensitivity of the nonconductive inner pipe liner has been the principal impediment to implementation for flow measurements in light-water reactors. Ceramic pipe liners are currently available for pipe diameters up to 30 cm. Full exploitation of electrode and magnetic field shaping also does not appear to have been performed to minimize the sensitivity to flow profile. The development under the INERI project involves application of advanced digital signal processing as well as state-of-the-art fabrication technologies for the ceramic liner. Given the early stage of development, progress should be monitored over the long term because this measurement technology has the potential to impact operating margins.

2.1.8 Fabry-Perot Fiber Optic Temperature Sensor

In recent years, the radiation tolerance of fiber optic sensors has been investigated to determine the prospects for potential applications for nuclear power plant measurements.⁸ In general, fiber optic sensors are immune to electromagnetic and radio frequency interference (EMI/RFI), so they can be used in strong EMI/RFI environments. Other potential advantages that fiber optic sensors provide are higher sensitivity, smaller size, less weight, larger bandwidth, and ease of

multiplexing. Therefore, if they can demonstrate sufficient environmental compatibility, they will be a promising new sensor type for measuring temperature in nuclear power plants. Ohio State University performed irradiation and other environmental tests on a commercially available Fabry-Perot fiber optic temperature sensor and documented promising results that indicated a level of resistance to the light losses resulting from external influences such as irradiation effects, high temperature, and pressure.⁹ Some degradation caused by mixed neutron/gamma irradiation effects was observed, but potential solutions were identified for further research.

Fabry-Perot fiber optic temperature sensors employ the Fabry-Perot interferometric sensing mechanism (which basically means that interference properties are used to precisely determine wavelength changes caused by thermal effects on fiber pairs in the sensor head). Interferometric fiber optic sensors are phase (or wavelength) modulated, and they have high accuracy and sensitivity and may be independent of the absolute light intensity transmitted or detected. Because of the potential performance benefits of these devices for temperature measurements, the progress in demonstrating the environmental compatibility of this technology should be monitored over the long term.

2.1.9 Optic Pressure Sensors

Pressure sensing at nuclear power plants is almost always performed through some form of elastic member deformation caused by a pressure differential. The deficiencies in nuclear plant pressure sensing are generally associated with either changes in the elastic performance of the member (softening due to increased temperature, radiation induced stiffening, corrosion product build-up, etc.) or with sealing the sensor across a pressure differential (leaking). The route that others have employed to avoid having to use a mechanical pressure differential to detect a contained pressure is to employ the internal pressure of a solid that is located entirely within the pressure being measured as the other side of the differential pressure. For example, changing the atomic lattice spacing, which in turn is altered by the applied pressure, alters the wavelength of ruby fluorescence. This type of pressure measurement technology is interesting, but some years away from any potential nuclear plant application.^{10 11} Alternatively, optical pressure sensors are available. Essentially, an optical path can be defined by a compressible medium with the relative state of compression of the medium changing the guiding characteristics of the path. However, the environmental compatibility for radiation environments associated with many safety-related measurements at nuclear power plants has not been definitely shown. Nevertheless, this sensor technology warrants monitoring to detect further development that could facilitate potential safety-related nuclear power applications.

2.1.10 Gamma Ray Tomographic Spectrometry

Component nondestructive examination in general and pebble-bed modular reactor (PBMR) fuel balls in particular can be advantageously performed using gamma-ray tomographic spectrometry. While PBMR fuel balls can be examined both during and after manufacture using an external X-ray source, newer technology would be useful for the auto gamma-ray examination of fuel balls that have cycled through the reactor core.

Fuel balls emerging from the reactor core are highly radioactive, emitting many X and gamma rays as well as delayed fission neutrons. Conceptually, a gamma-ray tomography instrument for PBMR fuel balls would involve a position-sensitive gamma-ray detector coupled to a collimating grid. While a traditional Anger camera would give some general fuel ball features, incorporating Compton gamma-camera technology and an advanced, coded aperture collimator would more easily produce a detailed coating structural picture.¹² A coded aperture collimator is a gray-scale coded shadow mask that functions as an efficient high resolution collimator. A Compton camera

uses the energy and time of two gamma events (Compton scatter and a photoelectric absorption) along with the kinematics of Compton scattering to back project the arrival angle of an incident gamma ray. This type of gamma-ray imaging technology is at the heart of modern gamma-ray telescopes. However, it has yet to be applied to nuclear power applications. The critical element required for large-scale deployment of this technology is improved cadmium zinc telluride (CZT) crystal production. The current production yields for spectroscopic grade CZT crystal production remain in the single digits. Currently these cameras are fabricated from a large number of individual CZT crystal elements that are further subdivided electronically. While scintillator detectors have been employed in some measurements, the wide range of incident gamma-ray energies makes the improved spectroscopic capabilities of a CZT detector important. Development of large spectroscopic-grade CZT crystals is important if this technology is to migrate eventually into safety-related applications at future nuclear plants.

2.1.11 Hydrogen Sensor

A unique hydrogen sensor was developed at ORNL under DOE and EPRI funding. This sensor has the potential for nuclear plant application in the near term (as a monitor for hydrogen accumulation in reactor systems) and in the long term (as an essential element of a nuclear hydrogen production plant). The basis for the sensor is a robust technique for measuring hydrogen in the environment by monitoring the resistance change of a material that absorbs hydrogen molecules. As hydrogen is absorbed into the material, the electrical resistance increases and this change can be measured and correlated to hydrogen concentration. Applying heat to the material, which purges the hydrogen and resets the sensing device, regenerates the sensor. This sensor provides detection over a broader magnitude of hydrogen concentration than almost any other commercially available technology. In addition, the sensor and its signal conditioning and output electronics can be housed in a small and robust package. The measurement range can be 0.5 to 100% H₂ with an accuracy of $\pm 5\%$. The response time is on the order of seconds, and the package allows the system to function in higher than ambient temperatures and under significant pressures. The status of this sensor should be monitored in anticipation of eventual nuclear power application.

2.1.12 Smart Sensors

Several instrument vendors have “smart sensors” on the market with range of features based on varying degrees of computational power. Some of these products offer dual outputs to accommodate the digital information (e.g., health, validity, quality, correction for nonlinearities or other known characteristics) while offering the option of accessing traditional analog signals. However, the trend is to develop communications according to one of the sensor bus or field bus standards, and the sensor market is being driven by large industries that do not face the same regulatory constraints as nuclear power. The time is approaching when “dumb” sensors may be costly or difficult to acquire. In the 1990s, one nuclear vendor devised a split architecture configuration that would allow the sensing element to be placed in harsh environments (e.g., containment) while permitting the microprocessor-based electronics to be situated in a separate, milder location. However, that product line was never developed as far as the prototype stage. Based on market considerations and the likely performance benefits smart sensors offer, it is reasonable to expect expanding use of this technology for nonsafety-related nuclear power applications in the near term and eventual migration of the technology into safety-related nuclear power applications. Thus, this technology should be considered for more thorough investigation in the near term.

2.1.12.1 Sensor Fusion

Sensor fusion is the process of obtaining information (such as more detailed process state or equipment condition knowledge) through the integration of data from multiple sensors of the same or different types. Usually, the result of sensor fusion is a model of a system or a subsystem that gives a user insight into the operation or performance of the system or subsystem. Significant work has been performed in this area over a number of years but, for nuclear power applications, the most significant techniques are referred to as redundant sensor monitoring and inferential modeling. For the purposes of this survey, inferential modeling is treated under diagnostics and prognostics. A prominent example of redundant sensor monitoring is EPRI's Instrumentation Calibration Monitoring Program (ICMP),¹³ which has been reviewed by NRC.

2.1.12.2 Enhanced Diagnostics

Sensors in optimum condition and performing as intended do indeed give a highly credible view of the operating conditions of nuclear power plants. However, the combination of environmental stress and time may degrade sensor performance, resulting in increasingly greater uncertainty about the plant condition over the course of an instrument's lifetime. Much of the value of smart sensors lies in their potential to diagnose and report their own condition (e.g., drifts and impending failures). These capabilities, however, rely on digital logic and signal processing and as such have not yet been extensively implemented at nuclear power plants, particularly in safety-related applications. This is a functionality of this technology that merits long-term monitoring.

2.2 Communications Media and Networking

Communications media (e.g., cables, fibers, wireless bands) and network systems provide the pathways by which data and information are distributed among the field devices, processing components, and display systems in a plant. To accomplish the survey in this technology focus area, a review of the current components, techniques, and approaches was conducted. In reporting the findings of this review, the information is organized according to an expanding view of network technologies that encompasses the range of topics from the architecture for interconnection platforms to the physical layer based on communications media to network protocols to network management to high-level network design approaches. Obviously, data communications represents an extensive technological focus area, and a general tutorial addressing all of its technical elements is beyond the scope of this report. Therefore, this section presents selected highlights from the technology that represent key advancements or expected developments and significant or evolving approaches.

In nuclear power, traditional direct-wired, point-to-point connections between analog equipment has been the norm. Recent years have seen the introduction of data networks serving plant personnel and some upgraded I&C systems. The advanced boiling-water reactors (ABWRs) in Japan and the most recent PWRs, such as the Electricite de France Chooz B, include substantial use of wired and optical communications networks. The current control and protection products on the market make use of specialized Ethernet or proprietary protocols for networked microprocessor-based or field programmable gate array (FPGA) equipment. Fieldbus standards are maturing, and networked field device are likely to see increasing application as part of I&C upgrades for plant life extension—with smart sensors becoming more prominent. It is to be expected that new plants, both the near-term and long-term deployment options, will take advantage of the advancements in communications technologies to facilitate highly integrated, autonomous control and information systems. In addition, future nuclear power plants may not necessarily have complete separation of safety systems from control systems (adapting lessons learned from the Chooz B design experience). In the mid-1990s, a utility owners' group developed design requirements for a plant communications "backbone." Segmented networks

provided the foundation to that concept with a safety-grade network connected to the remainder of the plant backbone through a one-way bridge.

2.2.1 High-Performance Architectures

A survey of communications media and networking trends would not be complete without some attention being directed toward the core multiplexing technologies that are the very essence of data movement, organization, and context switching. The highly specialized science of packet switching and control is key to the implementation of all networking implementation. This technology area is evolving as quickly as the more commonly recognized networking areas. For this reason this section begins with a discussion on how these architectures are expected to change.

Three emerging interconnection technologies are poised to radically change the way computers communicate with peripherals and each other. These technologies are RapidIO™, InfiniBand™, and the Intel® XScale™ microarchitecture.

RapidIO¹⁴ is an interconnect architecture designed to be compatible with the most popular integrated communications processors, host processors, and networking digital signal processors. RapidIO is a high-performance, packet-switched, interconnect technology. It addresses the industry need for high-performance embedded architecture that provides reliability, increased bandwidth, and faster bus speeds in an intra-system interconnect. The RapidIO interconnect allows chip-to-chip and board-to-board communications at performance levels scaling to 10 gigabits per second (Gbps) and beyond. The RapidIO architecture is an electronic data communications standard for interconnecting chips on a circuit board and circuit boards using a shared backplane. The RapidIO specification defines a high-performance interconnect architecture designed for passing data and control information between microprocessors, digital signal processors (DSPs), communications and network processors, system memory, and peripheral devices within a system. It is intended to replace current processor and peripheral bus technologies such as peripheral component interconnect (PCI) and proprietary processor buses.

InfiniBand¹⁵ is an emerging architecture for computer servers that may revolutionize how distributed systems are built, deployed, and managed. InfiniBand architecture enables greater server performance and design density while creating data center solutions that offer greater reliability and performance scalability by creating a centralized input/output (I/O) fabric. InfiniBand technology uses a channel-based, switched-fabric, point-to-point architecture.

As processor speeds increase with Moore's law and the Internet drives the demand for constantly available data, the biggest gate to improved overall performance is the I/O subsystem. InfiniBand architecture provides a blueprint for significantly improved performance and increased availability to meet the needs of the network interconnect. InfiniBand architecture offers three levels of link performance —2.5 Gbps, 10 Gbps, and 30 Gbps. InfiniBand architecture also enables low latency communication within the fabric, enabling higher aggregate throughput than traditional standards-based protocols. This positions InfiniBand architecture as the I/O interconnect for data centers and large integrated facilities. InfiniBand architecture enabled servers are expected to ship in the first half of 2002, and 50% of total servers are expected to be using InfiniBand architecture by 2005.

Intel® is developing a new architecture family called XScale microarchitecture.¹⁶ It will allow implementation of a wide range of Internet applications in a manner that achieves ultra-low power consumption with high performance processing. It is targeted for use with a broad spectrum of end products. These range from handheld Internet devices to enterprise Internet

infrastructure products, all of which can access and process rich content at all stages of the Internet. The microprocessor core can be surrounded by high-bandwidth PCI interfaces, memory controllers, and networking microengines to provide a highly integrated, high performance, I/O or network processor. The Intel XScale microarchitecture is designed with Intel's state-of-the-art 0.18-micron production semiconductor process technology. This process technology enables the microprocessor core to operate over a wide range of speed and power.

These architectural developments have the potential to impact the distributed computing and high-speed data processing capabilities that are likely to be prominent in the integrated, autonomous control and information systems at future nuclear power plants. These developments should be monitored and, as capabilities mature, investigated more thoroughly in terms of performance and reliability characteristics.

2.2.2 Network Physical Layers

2.2.2.1 Optical Networking

Tightly integrated optical computing and networking will eventually become a reality. Until that time, it is anticipated that significant improvement will occur in the capacity of fiber-optic carriers to handle increasing amounts of data. These technologies most probably will not be deployed at the desktop or server level, but rather as a main trunk data highway between geographic locations (e.g., for enterprise-wide networks). Current industry design efforts are focused on using GaAs integrated circuits (ICs) and InP optoelectronic devices for 40-Gbps components, but a shift to a more monolithic InP approach is expected for greater speeds. The merging of microwaves with optics is to be expected as higher and higher speeds are targeted. This development is likely to be crucial for achieving electronic time-domain multiplexing (TDM) at OC-768 (which is a standard used to define a level of network throughput equivalent to about 40 Gbps). Some of the commercial research and development for technologies that can provide 40 Gbps may also be suitable for 160-Gbps devices. Figure 2.4 shows how the technologies will probably evolve to meet the higher bit rates.¹⁷ As the data transport rate in fiber increases, the fiber-optic transmitter/receiver electronics will migrate to higher-speed platforms where suitable application-specific integrated circuit technologies will need to be developed in compound semiconductors with increased electronic carrier mobility. InP-based compound semiconductors possess the highest mobility and are also well suited for telecommunication optical components.

Another development of interest in fiber-optic communications technology is the introduction of tunable lasers into the telecommunications industry to enhance flexibility and reliability of optical networks. Current fiber optic technology allow single fiber-optic strands to carry multiple wavelengths of infrared radiation across entire continents, with each wavelength channel carrying digital data at high bit-rates. Known as wavelength-division multiplexing (WDM), this process greatly expands the capacity of fiber-optic communications systems, making them one of the most important parts of the foundation on which the Internet relies. A typical 176-wavelength system uses one fixed laser per wavelength. Tunable lasers can provide redundancy and flexibility at multiplexing locations by letting carriers remotely reconfigure wavelength channels as needed. Thus, tunable lasers can make possible dynamically reconfigurable optical networks as well as optical switches.

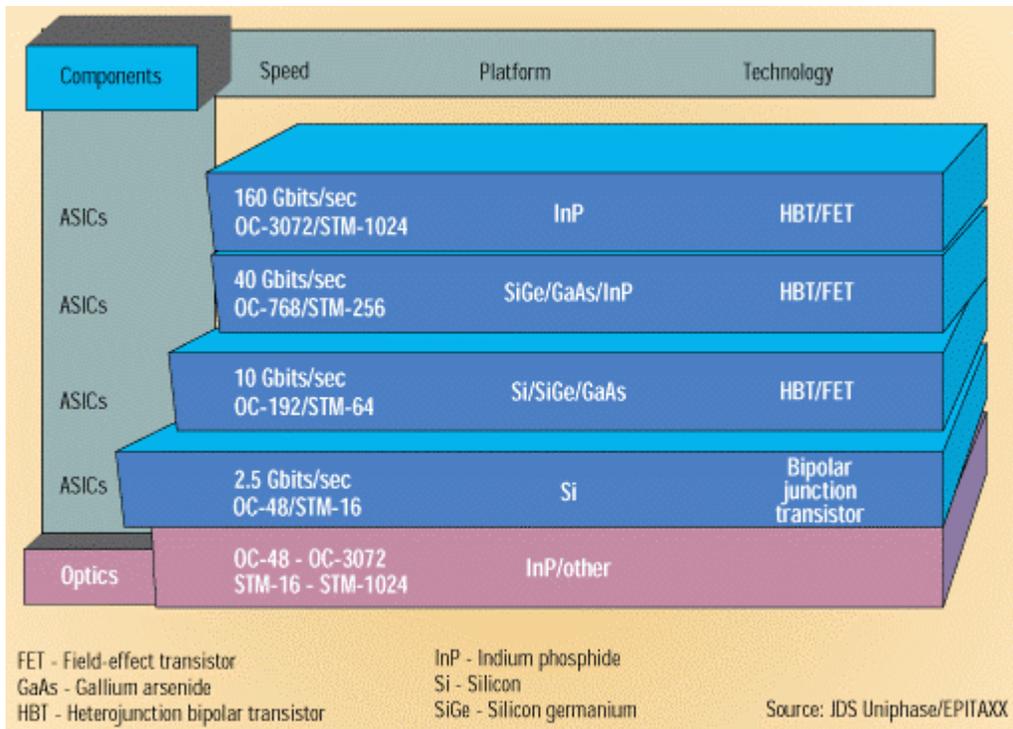


Figure 2.4. Expected progression of fiber-optic transmitter/receiver electronics.

Generally, tunable lasers are likely to be applied in situations in which large bandwidths are required, such as in the telecommunications industry. However, laser technology can be used for reliable point-to-point optical communications. Therefore, their conceivable application for nuclear power might be to provide redundancy for a wireless (in this sense, open space) optical communications link. If the primary link fails (for example, some organic vapors are known to cause optical transmissions in certain frequency bands to fail), the tunable-laser-based backup can transmit on another available frequency. However, given the sensitivity of such links to moisture and vibration, the application opportunities would probably be limited to controlled environments.

Fiber-optic communications will probably see increased use in nuclear power applications. However, the data throughput needs envisioned for even the most highly integrated control and information systems within a nuclear plant should be well within the current scope of the technology. The biggest challenge for safety-related applications to the field-device level appears to be environmental compatibility for fiber-optic carriers. NRC has investigated fiber-optic communications in the past and should continue to monitor the state of the technology.

2.2.2.2 Wired Networking

Wired communication technology is evolving to satisfy increasing needs for higher bandwidth. Copper-based networking offers advantages for local interconnections because its cost is lower than that of fiber-optic carriers, and it can already support gigabit Ethernet and 155 megabits per second (Mbps) asynchronous transfer mode (ATM) protocols. Copper-based networking also offers discipline because it is a controlled medium; whereas, wireless is still an immature technology. However, Category 5 cabling will be challenged by other networking options and the consumption of more of the available bandwidth by higher-speed computing technologies. The Gigabit Ethernet Alliance has concluded that this evolution in computing technology will have a

significant impact on cabling. More stringent high performance standards for copper wire technology are expected to help address this need. Obviously, these trends could impact implementation choices for long-term deployment and should be monitored.

2.2.2.3 Wireless Networking

The exploitation of wireless networks for digital data applications is expected to accelerate with the introduction of different high-speed networks. Carriers in Japan are beginning to deploy the so-called 3G technology, or third-generation wireless cell phone systems. This technology is being introduced in Europe and should see applications in the United States in 2003. Unlike the previous two generations of cellular networks, 3G systems have been designed from the beginning to carry data as well as voice. Carriers promise downloads approaching 2.4 Mbps. This is twice as fast as wired broadband services and more than adequate to saturate cell phones, handheld devices, and laptops with streaming video, music, and real-time interactive games.

In the telecommunications industry, two main standards compete for market dominance. It is expected that Europe and Asia will convert from the global standard for mobile communication (GSM) to wideband code division multiple access (W-CDMA). In North America, carriers who use code division multiple access (CDMA) networks, such as Sprint and GTE, will also migrate to W-CDMA. Other carriers who use time division multiple access (TDMA) systems, such as AT&T and Southwestern Bell, plan to go to enhanced data rates for global evolution (EDGE). EDGE requires relatively minor infrastructure upgrades, but it is slower and has a theoretical maximum data rate of 384 kilobits per second (kbps). W-CDMA is much faster at 2 Mbps.

Other technologies are also poised to add their contribution to the overall wireless evolution in communications. More sophisticated antennas are under development that combine advanced designs with digital signal processing. These are referred to as “smart antennas.” In addition, ultrawideband (UWB) technology is moving from the laboratory to the field.

Benefiting from the advances for the telecommunications industry, industrial processes are going wireless. However, unresolved issues remain. One issue is that wireless systems must be able to withstand harsh industrial environments—both the physical environment and electromagnetic compatibility (EMC). Another issue is that manufacturers have yet to settle on standard architectures and protocols, making most of the wireless systems incompatible with each other. As a result, after a product line is selected, communications system expansions or component upgrades will probably be limited to single-vendor options to avoid incompatible, isolated systems or the need for a complete communications systems replacement. A third issue is the power required for existing wireless systems, that is, wireless equipment typically requires large, high-density power sources to run for any period of time.

Nevertheless, progress is being made in all of these areas and wireless systems will inevitably be used in numerous applications in industrial plants. Figure 2.5 illustrates some probable applications. Conditioning of the wireless system for the expected environment (physical or electromagnetic) can be achieved in the design stage and verified through environmental testing. Also, the trend in industrial and business wireless architectures and protocols is moving away from proprietary systems toward open standards. IEEE 802.11 is the standard of choice for wireless local area networks (LANs), and Bluetooth is the preferred standard for linking wireless office devices (printers, faxes, etc.) together. Presently, the IEEE 1451 Committee is developing a wireless standard for smart sensor buses, and it probably will become a de facto open standard for sensor systems, just as IEEE 802.11 is for wireless LANs. Also, low-power electronics, made possible by the introduction of new submicron semiconductor processes and power management techniques, are being incorporated into industrial wireless systems. This means that in the future a

wireless system may be able to operate for extended periods with only a button-cell battery. The future trends for industrial wireless systems include:

- Increases in bandwidth, computing power, and timing resolution will enable increasing scientific refinements of processes;
- Support of open communication standards will enhance both networking efficiency and network security;
- Increased integration of inventory control using radio-frequency identification (RFID) tags and sensor networking will occur;
- Reliance on administrative controls and engineering designs to help prevent surreptitious “attacks” from outsiders will continue (whether over-the-air or over-the-net);
- Growing use of network diversity and segmentation will help prevent attacks from within; and
- Adherence to good engineering design practices and administrative controls will minimize the potential for EMI upsets.

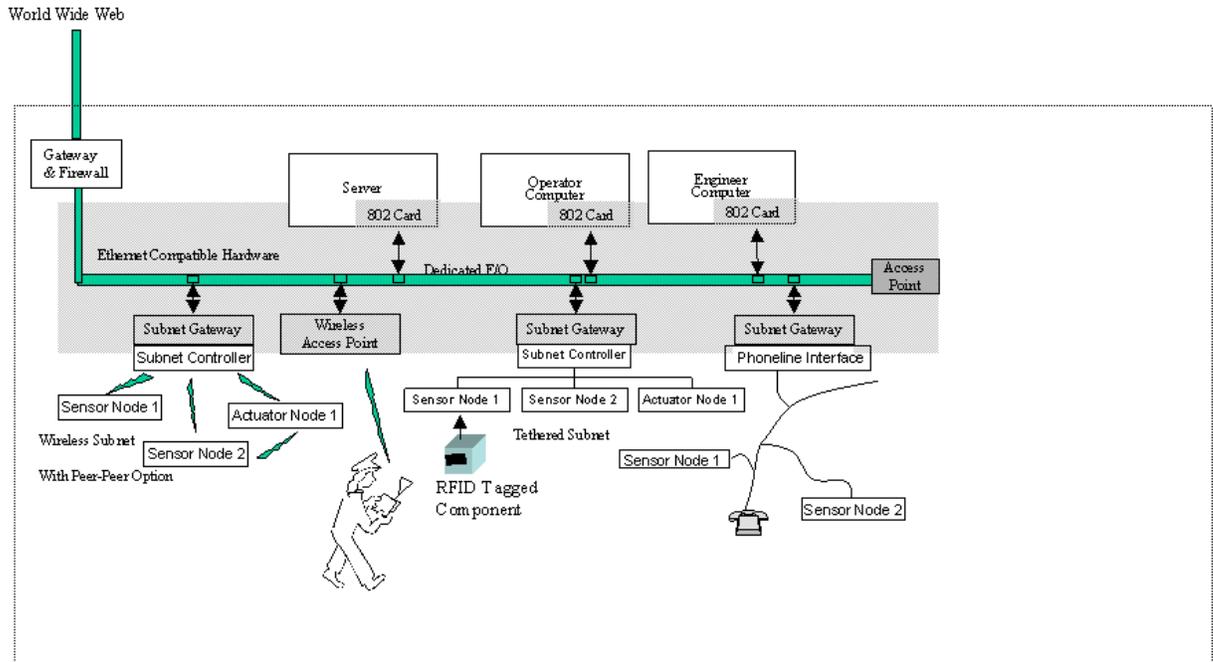


Figure 2.5. Illustration of potential wireless system applications.

These technological advancements described in this discussion will lead to greater use of wireless technologies in industrial applications. Sensors and applications used as mobile agents will create

new flexibility and costs savings for some industries by liberating them from the costs and constraints of wired connections. This is particularly relevant given the desire to minimize the up-front costs of future nuclear power plants. Issues related to security and compatibility when considering wireless networking will continue being addressed. Of necessity, some applications will not be likely candidates for wireless communications because of the need for guaranteed, certain security and the real discipline offered by a wired network. However, even these may see wireless interconnection used for some peripheral connections such as printers and scanners. The NRC has already begun research into wireless technology that is migrating into balance-of-plant and business applications within nuclear power plants. Based on the rapid pace of advancement and product development for this emerging technology, this research is timely.

2.2.3 Safety-Related Fieldbus

Approximately 60 fieldbus systems are in use despite attempts to develop an international standard. No consensus has yet developed on the right way to network instruments. Instead, consortia are developing their own solutions and letting the marketplace decide the winners. At the same time, systems are guiding development towards some common ground: communications application-specific integrated circuits (ASICs) are common, high-speed Ethernet is being implemented, and more effort is being made to provide precise and deterministic bus timing in order to support control loops and safety actions. Given the current state of competitive pressure among the vendors, it seems inevitable that fieldbus systems will adapt networking developments occurring for general computer systems and telecommunications. The result may be that fieldbus systems adopt general computer industry standards for bus communications, simply adding their own higher layers of messaging to support control applications.

International examples of fieldbus networks have received safety certification. Echelon's LonWorks networks have been accepted by Gosatomnadzor (GAN) for safety-related application at two Russian nuclear power plants. The Gardia-2 Safety System, by DICS Intertrade of Sophia, Bulgaria, uses a triply redundant LonWorks network in its control and diagnostics of safety valves for pressurizers and steam generators. The systems have been in use since early 1999 at Units 1 and 2 of the Kola Nuclear Power Plant and since June 1999 at Unit 4 of the Novovoronezh Nuclear Power Plant. The systems were certified by Groupe SEBIM of France to meet Class E1/K3 (French RCCE code) and ANSI/IEEE 323 and 344 safety standards for nuclear power electric generating plants. The system uses special voting algorithms, redundant power supplies, and extensive diagnostic routines to ensure that the system remains on-line at all times.

In recent years, NRC has conducted a survey of fieldbus technologies.¹⁸ It is expected that networks for field devices will be the norm for control and information systems in new plants. The technological evolution of the sensor market and industry's desire to reduce cabling costs are expected to drive the nuclear industry in that direction. As a result, near-term research into the safety characteristics of fieldbus technologies seems warranted. Because safety considerations are the primary concern for nuclear plant applications, an overview of safety fieldbus options is included in this discussion.

Several approaches to safety fieldbus networks are being implemented in specialized industrial applications. These include the introduction of several new names in this field, including Interbus, Safenet, Esalan, and DeviceNet Safety.

Although safety fieldbuses are not yet widespread throughout the manufacturing industry, they are already being used in some plants, and they will likely be installed at an accelerating rate as confidence in the technology increases. Pilz is no longer the only supplier working in this field:

networks based on Interbus, Profibus, and AS-Interface are now available, as well as the Safenet and Esalan systems. Another that has only recently been announced is based on DeviceNet.

The DeviceNet Safety system, in common with Profisafe and Interbus Safety, will allow users to mix conventional and safety devices on the same network. Clearly, no industry consensus exists yet on whether this is a good or bad practice, and not enough systems have been installed to determine which approach customers prefer. Many of the various safety fieldbuses have the support of some of the largest suppliers of automation and control equipment, and because the development cost was probably very high, it is unlikely that any of these will disappear in a hurry. Users may have to work through a complex selection process for many years to come.

The debate continues over whether the use the same cables for power and data is acceptable, or whether the same network should carry both safety and nonsafety data, but few would deny that safety fieldbuses have their attractions.¹⁹

Three prominent fieldbus systems will be discussed here. Each of the following systems has European origins and has been developed with factory safety applications as a primary goal.

- AS-Interface bus with the “Safety at Work”²⁰ enhancement,
- ProfiSafe, an adaptation of the Profibus system,²¹ and
- SafetyBus,²² based on a safety-grade programmable logic controllers (PLCs) and the controller area network (CAN) bus.

The discussion will also address another approach to safety-related applications of fieldbus. This involves installation of a standard fieldbus system with enough redundancy, fault isolation, and diversity to achieve the required reliability and availability.²³ In this case, a fieldbus system must be chosen that allows such configurations.

2.2.3.1 AS-Interface

AS-Interface is a low-cost electromechanical connection system designed to operate over two-wire cables. The cable carries data and power over a distance of up to 100 m. Repeaters can be used to accommodate longer distances. AS-Interface is especially suited for lower levels of plant automation. Examples include binary operated devices such as switches that need to interoperate in a stand-alone local area automation network controlled by a PLC or personal computer (PC).

An AS-Interface semiconductor device has been developed for facilitating the integration of user modules and field devices. This should help limit the costs of implementation and improve conditions for a robust and interoperable environment. The primary applications area for this technology is the networking of binary sensors and actuators. These are typically used in safety-oriented applications. An overview of the design for AS-Interface Safety at Work is described online (also, see Fig. 2.6). The online description reports:

The concept enables applications up to safety Category 4 according to IEC61508 and has been accepted by German certification bodies TÜV and the BIA (Berufsgenossenschaftliches Institut für Arbeitssicherheit). The Safety Monitor was formally approved in 2001 Q2 and Safety at Work products are now (mid-2001) being installed and tested.²⁴

AS-I technology has been implemented at several major industrial plants (automotive and semiconductor). While these applications are proprietary in nature, specific reference are available on

the Web about Toyota, Honda, and a semiconductor and printed circuit board (PCB) components manufacturer having systems installed with up to Category 4 of EN954-1.

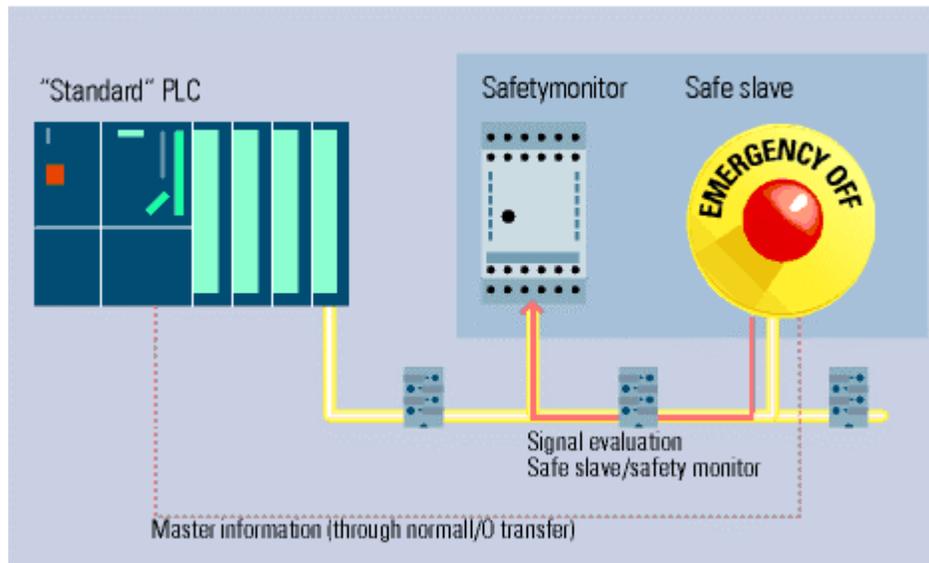


Figure 2.6. Safety at Work: AS-Interface as safety bus.²⁵

2.2.3.2 ProfiSafe

ProfiSafe is a profile or way of operating on the ProfiBus (see Fig. 2.7). It can be referred to as a communications profile. Only limited hardware is capable of operating with ProfiSafe (the Simatic S7-400F Fail-safe PLC from Siemens), so it is not clear whether it is widely used. An extensive Internet search did not identify any explicitly documented cases on the use of ProfiSafe.

In a recent speech at conference in Erlangen, Germany, Klaus Werner Stellwag of Siemens described a ProfiBus profile for safety-critical applications.

Siemens has made it possible to transfer safety-related signals using a standard bus. To accomplish this, the ProfiBus was upgraded to include the ProfiSafe telegram, thus enabling all process and safety-related data in decentralized plants and machine components to be completely available using a bus cable. Only Siemens Automation and Drives offers a complete product range of drives and control systems for machine tools that can communicate using ProfiSafe.²⁶

MESCO Engineering²⁷ also provides an important perspective on ProfiSafe. MESCO claims ProfiSafe fulfills all technical requirements for fully decentralized solutions in the field of safety technology. ProfiSafe eliminates the need for special fieldbuses and allows for safety-relevant automation solutions over the standard ProfiBus. Operators benefit from simpler cabling, a uniform electronic design and consistency as regards specific parameterization and remote diagnosis. ProfiSafe sets new standards in safety technology.

A useful introduction to ProfiSafe can be found online in the publication Connection.²⁸ Members of the working group responsible for defining ProfiSafe are Festo AG, Hima GmbH & Co. KG, Kloeckner-Moeller GmbH, Leuze Lumiflex GmbH & Co., Schmersal GmbH & Co., Sick AG, Siemens AG, University of Munich, and Wago GmbH. A variety of safety standards (e.g., IEC

61508 Base Standard for Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 60204-1 Electrical Equipment of Industrial Machines...) are satisfied to allow ProfiSafe to be used in a large number of applications.

A good technical summary of ProfiSafe can be found online²⁹ in an article from Control Engineering, Europe, 2001.

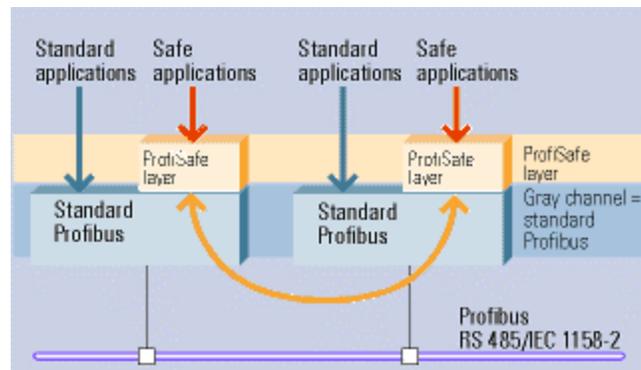


Figure 2.7. Diagram showing application deployment with ProfiSafe and Profibus technology.³⁰

2.2.3.3 SafetyBus

An example of the application of SafetyBus can be found online.³¹ In this reference, machine safety is emphasized:

The Warwick Manufacturing Group, manufacturers of aerospace and automotive components based in England, installed SafetyBus to offer machine safety. This was presented in two separate robotic cells—Warwick Automation Research and Evaluation System (WARES) and Flexible Tooling System (FTS). The WARES facility was for examining new manufacturing technologies and agile control system strategy research.

Honda Engineering, the automobile manufacturer, is using SafetyBus P in its Swindon plant for safety control and diagnosis of a three-robot test cell. This has helped to increase the flexibility of the assembly line and minimize cabling costs. SafetyBus P has been installed in the Seoul airport for safety-control functions, which cover a large area.³²

SafetyBus is also used for building fire protection and smoke extraction at an installation in Dusseldorf.³³

2.2.3.4 Foundation Fieldbus

Foundation fieldbus has been employed in safety-related applications through redundant implementations. As an example, Deten Chemicals S.A. produces a raw material used in detergents at its plant in Camacari, Bahia, Brazil. A Foundation fieldbus system was installed by Smar to handle some of the controls. Both redundant communications and redundant bus power

systems were used for critical controls. This included fieldbus communications between PLCs and a motor control center (MCC) that has its own PLC.

Another example occurs at the Corning's Concord, North Carolina, plant, which has over 600 analog devices and over 2000 discrete points running over a Foundation fieldbus system. It is a fully redundant design with the aim of achieving high reliability and availability. Each bus segment is powered from both ends of the bus. On each end of the bus segments is a bus interface card attached to redundant I/O servers. The I/O servers have redundant Ethernet cards and send their data to redundant data servers. There are also redundant Ethernet fiber switches. The system includes 16 operator consoles.

2.2.4 Network Security

The primary means of securing networks are by limiting access and encryption. Limiting access includes the use of access control lists in network hardware, deployment of firewalls with properly configured rule sets, physical security, and user authentication. Intrusion detection is used in conjunction with limiting access to determine whether a security breach is occurring or has occurred. Encryption, in the network sense, is accomplished with either direct hardware encryption of all network traffic or through the use of virtual private networks (VPNs).

Advancing and emerging technologies related to network security fall into several areas: wireless network security, advanced data analysis techniques for intrusion detection, simplified deployment for public key infrastructure (PKI), improved biometric authentication accuracy, increased key size, and algorithm development for VPN encryption.

Although current wireless network products have security features, significant flaws in their design have been identified, and more work will be needed in the near future to make them truly secure. A report by Chalmers University gives a detailed comparison of wireless network products and a discussion of their security.³⁴ Intrusion detection for wireless networks has only recently become available. Internet Security Systems, an industry leader in intrusion detection, has wireless security information online.³⁵

Current commercial intrusion detection products have limited capability to detect sophisticated attacks via seemingly random information gathering over an extended period of time. Research is continuing in the development of advanced data analysis techniques necessary for agile systems to identify these more covert threats. A review of some of these techniques can be found online.³⁶

The technology of PKI with digital certificates is well developed and simple to use. PKI it is not in widespread use, however, due to the planning required for initial deployment and the lack of PKI-aware applications. Within the next few years, efforts³⁷ are planned to simplify and streamline the initial deployment process and to convert more applications for use with PKI.

Current biometrics research³⁸ is directed toward improving overall accuracy and determining the appropriate level of biometric technology for a given application.

The current state of computer security uses 128-bit keys for VPNs, but an increase to 1024 bits is expected within the next 10 years. Work also continues in the development of new algorithms for encryption.³⁹

In addition, the security of most computer and network products are currently transitioning from evaluation using the U.S. Orange Book (i.e., DoD Trusted Computer System Evaluation

Criteria)⁴⁰ to that using the Evaluation Assurance Levels (EALs) of the common criteria that were developed in cooperation with the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and others. Products evaluations are based on comparison to the EALs using a protection profile. In the United States, protection profiles are primarily developed by the National Security Agency. The specific protection profiles to meet the EALs, especially for high security applications, are still being developed.⁴¹

In light of increased security awareness and the introduction of wireless communications into process control systems, recent research by NRC into the network and computing security is well justified.

2.2.5 Network Management

Network management is key to providing reliable network services. Not only must a network be designed with sufficient care in areas such as redundancy and protection, but the system also must be managed properly to allow high availability. Management capabilities include the following: topology monitoring, performance measures, error collection, link statuses, analysis capability, remote device control, alarming, and logging.

While many network devices include capabilities such as web or terminal-based management, network management refers to the ability to manage the entire collection of devices and links. The most common model for network management is one that consists of a collection of network management stations and network elements. Network management stations are typically workstations and network elements consisting of a wide variety of devices and software entities such as switches, end nodes, routers, virtual private network appliances, and databases.

For small networks, device-level management alone may be sufficient. Manageable devices such as routers, switches, hubs, and end nodes usually have one or more of the following management options: serial terminal port, telnet service, and web server. Any of these interfaces may be used to configure and monitor a single device or group of devices that the manufacturer may have integrated for management as a single entity.

Network-level management solutions consist of software that communicates with the managed devices and applications and nodes dedicated to the specific job of network monitoring (sniffers). Most network management software and devices uses the simple network management protocol (SNMP) discussed in RFC1067.⁴² All major network equipment vendors offer a software-based management solution for their equipment. However, vendor-specific solutions do not usually work well in a network using equipment from multiple vendors. Other vendors offer software-based management solutions that are equipment independent. High-end commercial management solutions tend to be expensive and require significant effort to configure and use. Recently, a lower-cost solution became available through the OpenNMS⁴³ project. The aim of the OpenNMS project members is to greatly reduce the cost of deployment and ownership while creating a highly customizable product that can fit the needs of the users.

Again, the trend toward highly interconnected, distributed computing systems for autonomous control of complex process systems suggests that the capabilities of network management solutions probably will have to be considered in the assessment of safety-related control and information systems for future nuclear power plants.

2.2.6 Network Design

Network design configuration issues include segmentation and routing topology, switching configuration, redundancy design, physical link selection, and layer-4 switching service use. The trend is for networks to be segmented into manageable sections with switching routers to control traffic flow between segments. This isolates local traffic, provides efficient traffic flow, and allows better management.

In the past most routing was performed by general purpose computing elements, now routing at levels 2, 3, and even 4 can be performed at wire speed. Layer 4 switching allows multiple nodes to provide a service that looks like a one-source service to the clients. For example, layer 4 switching may be used to create a virtual cluster of storage devices into one virtual server to improve performance and reliability. One vendor is now promoting a solution called XRN (eXpandable Resilient Networking)⁴⁴ that consolidates the functions of link aggregation, redundancy, routing updates, and management for a distributed group of layer 3 switches. This allows a group of independent switches to be managed by a distributed core switching solution.

For systems requiring very high reliability, redundant links and dual-homed end nodes are used to provide communication that is tolerant of any single-point failure. The physical layer (i.e., transmission medium) is selected for compatibility with the environment. For example, fiber optics are the preferred choice where EMI/RFI or grounding problems exist. While the Ethernet physical layer is the dominant interconnect medium used in most local area networks, new technologies such Sonnet are available for special needs.

Other recent changes in network capability include the off-loading of network processing to network interfaces. With gigabit speed links, Internet protocol (IP) checksums must be off loaded to the interface to deliver high performance. Encryption and higher-level protocol functions may also be off loaded. Another example of off-loading processing is the use of network interface cards to operate a firewall. The use of network interface card (NIC) firewalls reduces the chances of intrusion and also shifts the processing load from the main processor. Use of network interface processing is also finding application with storage area network (SAN) over IP protocols where performance is critical.

Evaluation of emerging network design approaches may become an important consideration in the review of future power plants with highly interconnected, distributed computing environments for autonomous control and information systems. The trends in network design should be monitored, in particular, configuration approaches for high network availability and the robustness of high-speed switching routers and network interface processing.

2.3 Microprocessors and Other Integrated Circuits

This technology focus area consists of microprocessors, PLCs, FPGAs, DSPs, embedded microcontrollers and microelectronics. The periodic release of succeeding generations of microprocessors provides evolutionary rather than revolutionary changes in IC technology. Therefore, this survey does not address the latest series of microprocessors from the major manufacturers as emerging technology nor describe conventional IC fabrication technologies. Instead, the survey targets notable developments in IC capabilities (e.g., environmental compatibility), implementation approaches, and innovative circuitry.

For a variety of reasons, the nuclear power industry has been slow to adopt digital technologies in general. For nuclear plant safety systems, product lines have evolved from discrete analog components to general-purpose microprocessors to PLCs. More examples of microprocessor,

PLC, and microcontroller applications for control systems exist, especially in balance-of-plant and auxiliary system applications. An extensive awareness of issues regarding ICs at NRC also exist because of I&C system upgrades over the past decade. Nevertheless, the semiconductor industry responds to markets other than the nuclear industry, and obsolescence of IC product lines is rapid. Because great economic incentive drives the use commercial off-the-shelf (COTS) equipment, the nuclear power industry will probably see new IC technologies migrate into safety-related applications in the long term.

2.3.1 Radiation-Hardened Integrated Circuits

In high-performance, power-limited electronic systems, metal-oxide semiconductor (MOS), and ICs, particularly those of the complementary form (CMOS), are often employed for applications such as battery-powered computers, robots, timers, and embedded controllers (e.g., in many industrial and automotive applications). A primary feature of CMOS that is responsible for this prevalence is that the power consumed by CMOS logic elements is extremely low compared to nonvolatile metal-oxide semiconductor (NMOS) or bipolar circuits. In addition, CMOS inverters employ voltage signals that can be made highly immune to noise (i.e., they have a high noise margin). The combined features are uniquely suited for advanced data-handling and control systems in severe and remote environments.

Typical computing platforms—workstations such as PCs, PLCs, and FPGAs—rely on CMOS technology. The trend in computing and digital I&C circuitry is toward small feature-size (<0.25 μm) CMOS. The push for integrated-circuit processes with small feature size has resulted in high processing speed, but more important for nuclear plant applications, they have higher radiation tolerance. The thin gate oxides used in the current submicron processes are showing very good tolerance to ionizing radiation. Doses in the tens of Mrad have been shown to produce only small effects in operation.

The state-of-the-art of radiation-hardened (rad-hard) electronics and their suitability for the nuclear power plant environment may be gauged by the requirements and use of such systems in space applications. Space processors are being implemented for operation in a highly variable radiation environment. Variation with time and orbit is highly modulated by solar activity and the location of the space vehicle with respect to the radiation belts. The response of processors to solar flares may limit the applicability of commonly employed mitigation techniques such as triple-modular redundancy in modern microelectronics. As the technology migrates to smaller feature size, higher performance, and lower power, the sensitivity to single-event effects (SEE) of galactic cosmic rays (GCR) and protons increase dramatically to the level that necessitates the development of rad-hard ICs for space applications.

Three generations of rad-hard microprocessors have been developed and have qualified for space flight. Each generation offers an order of magnitude increase in performance (e.g., speed and computational capability) over the previous generation. The generic VHSIC space-borne computer (GVSC), a 16-bit microprocessor, is a multichip implementation of the U.S. military 1750A architecture fabricated in 1.0 μm /0.8 μm rad-hard CMOS. The RAD6000 is the first 32-bit space microprocessor based on the IBM RS/6000 Power Architecture. It is fabricated in a rad-hard 0.5 μm CMOS. As of October 2001, 278 rad-hard processors (GVSC and RAD6000) are operating in space onboard 86 separate platforms. The last and most modern microprocessor for space is the RAD750. It is a fully licensed, certified Power PC 750. It is fabricated in a radiation tolerant 0.25 μm CMOS process and is targeted for migration to an even finer fabrication process (i.e., 0.18 μm). The RAD750 currently operates at 133 MHz, offering 240 million instructions per second (MIPS) performance.

With the move toward smart sensors and sensor networks, the availability of electronics for harsh environments at nuclear power plants (i.e., containment) will probably become an issue. The trends in IC technology should make microprocessors, PLCs, and FPGAs available for containment application in the long term. Near-term application is less certain. Therefore, it is probably sufficient to monitor the development of rad-hard IC technology for space applications and maintain awareness of potential improvements in the radiation-tolerant characteristics of commercial ICs.

2.3.2 System on a Chip

Recent trends in miniaturization of circuit features and higher transistor density have resulted in development of the system on a chip (SoC) concept, in which most or all of the circuitry required for a system (e.g., a cellular telephone) can be contained on a single IC. These SoCs often contain analog, radio frequency (RF), and mixed-signal components to satisfy the growing demands of telecommunications applications (see Fig. 2.8). In contrast with conventional IC design, for which the entire IC will be designed by one company, SoC designers often need input from intellectual property providers that design circuit modules for use with other SoC circuit elements.

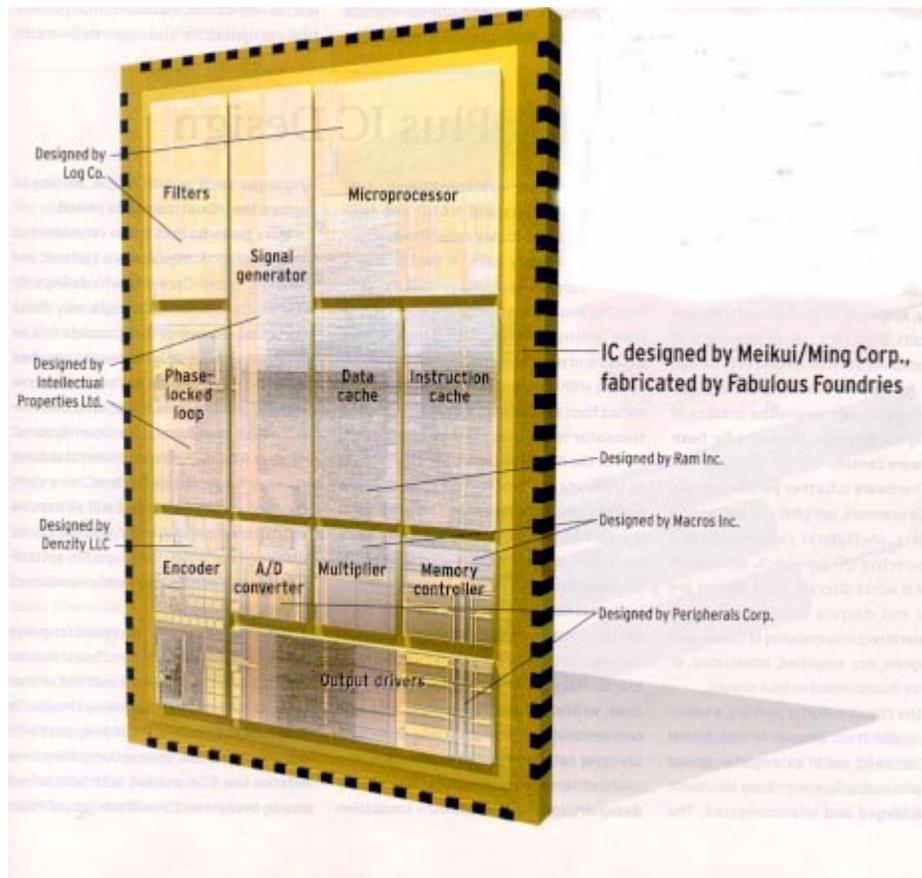


Figure 2.8. Hypothetical subsystems on a prototypical SoC. Different modules are typically designed by different intellectual property providers.

SoCs unite multiple subsystems, enhancing performance while saving circuit board space and power. In 1995, SoCs had hundreds of thousands of gates, a single programmable microprocessor core, and on-chip memory. Today, the digital, analog, and RF functions found on a single chip are far more diverse. For example, the super optical-disk controller for digital versatile disc (DVD) systems, developed by Matsushita of Osaka, Japan, combines the contents of three chips in one, reducing the power and space requirements while more than doubling playback speed. A simple yet innovative example of a SoC for sensing applications in remote or potentially hazardous environments is the bioluminescent bioreporter integrated circuit (BBIC) developed at Oak Ridge National Laboratory (ORNL). The BBIC is a miniature optical application-specific integrated circuit (OASIC) that consists of the sensing element, signal conditioning, signal processing, and wireless communications subsystems (see Fig. 2.9). The BBIC contains genetically engineered bacteria on the chip that emit blue-green light when they encounter a pollutant that they ingest as a food source. The light is detected by chip electronics (i.e., light is absorbed by the silicon, which induces electrical charges), and the resulting electrical signal reveals the identity and concentration of the pollutant. The resulting information is then transmitted for notification or alarm.

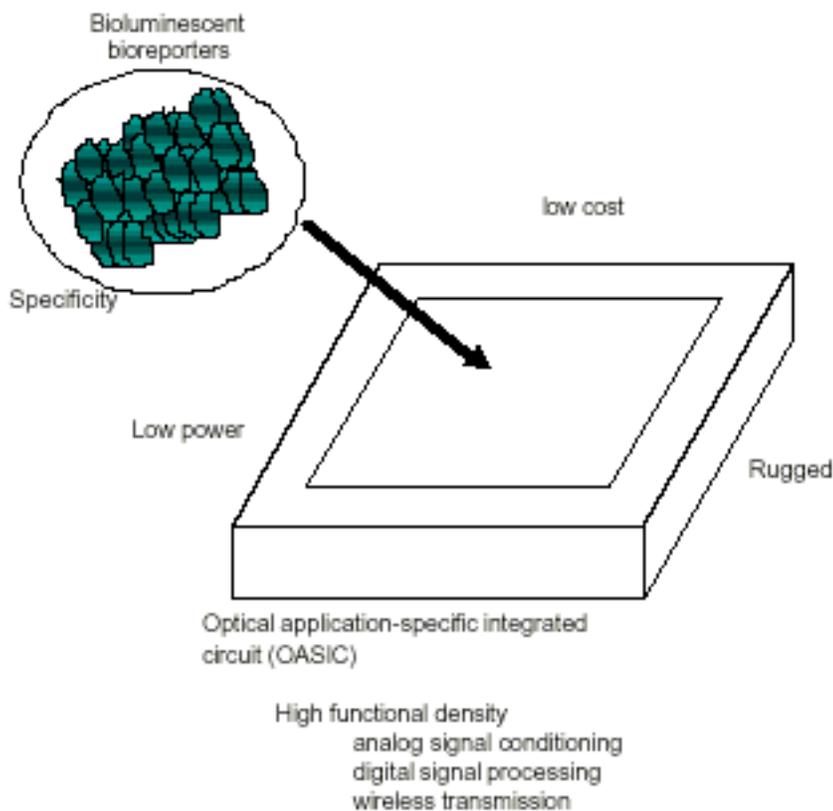


Figure 2.9. Attributes of BBIC.

SoCs could eventually lead to sensors on a chip applications that could be located in harsh environments and changed out (perhaps robotically) on a periodic basis. This would facilitate the addition of new measurement or monitoring capabilities at remote or harsh locations over the lifetime of a nuclear power plant without requiring expensive cabling or qualification for an

extended life. Currently, specialized applications are the focus of SoC development, so monitoring the long-term trends in this area would seem appropriate.

2.3.3 Optical Processors

Entirely optical computers will not be possible until some time in the future. However, electro-optical hybrid computer components are available today and have been possible since 1978. In particular, optical digital signal processors (ODSPs) are being developed and demonstrated in anticipation of near-term commercialization. However, it is uncertain when the technology will become widespread and demonstrate sufficient maturity and cost-effectiveness to facilitate safety-related nuclear power applications of such processors.

Optical computing was a hot research area in the 1980s, but the work tapered off because of materials limitations that seemed to prevent optical chips from getting sufficiently small and cheap to ever be more than laboratory curiosities. New conducting polymers can now be used to make transistor-like optical switches that are smaller and 1000 times faster than silicon transistors that are currently used in computers. Optical data processing can perform several operations simultaneously (in parallel) much faster and easier than electronics. Multiple frequencies (or different colors) of light can travel through optical components without interference, allowing photonic devices to process multiple streams of data simultaneously. This “parallelism,” when associated with fast switching speeds, would result in staggering computational power.

Optical interconnections and optical ICs have several advantages over their electronic counterparts. They are immune to EMI and free from electrical short circuits. They have low-loss transmission and provide large bandwidths (i.e., superior multiplexing capability able to communicate several channels in parallel without interference). They also are capable of propagating signals within the same or adjacent fibers with essentially no interference or cross talk.

The advantages of all-optical components notwithstanding, most optical components that are readily available are electro-optical (EO) hybrids, which are limited by the speed of their electronic parts. In the future, all-optical components will have the advantage of speed over EO devices, but currently there is a lack of efficient nonlinear optical (NLO) materials that can respond at low power levels. Almost every current all-optical component requires a high level of laser power to function as required. However, one vendor, Lenslet Labs, claims that its optical-based transform engine, optical digital signal processing engine (ODSPE), is capable of EO conversions at speeds of giga-vectors per second and greater and will be included in off-the-shelf, low-power products in the future.⁴⁵ The role of nonlinear materials in optical computing is extremely significant. Nonlinear materials are those which interact with light and modulate its properties. Several optical computer components require efficient nonlinear materials for their operation. What restrains the widespread use of all optical devices is the inefficiency of currently available nonlinear optical materials, which require large amounts energy for responding or switching.

Optical interconnections (i.e., EO hybrids) have been implemented in nuclear power plants as part of fiber-optic communications links. However, safety-related applications of optical processing seem unlikely in the near term. Given the potential increase in computational speed promised by optical ODSPs, it seems likely that such technology will eventually migrate into nuclear plant applications in the long term. Therefore, awareness of this technology should be maintained.

2.3.4 Vertically Stacked Integrated Circuits

Moore's law predicts that the steady growth in silicon-based IC complexity on which the information technology industry depends is approaching physical limits. Currently, microprocessors are fabricated on a single layer of silicon, much like a one-story building. The Pentium 4 processor, a state-of-the-art chip, has seven layers of wiring, but only on the bottom layer of pure silicon do the active semiconducting regions lie. However, a new approach of "three dimensional" IC design offers a possible means to increase transistor density. In this design, active semiconducting layers are stacked on top of each other, much like a skyscraper building. This builds upon the industry expertise in wafer design and could reduce manufacturing costs tenfold in comparison to traditional ICs. In the semiconductor industry, advanced chip technology is usually introduced in memory devices first. It is expected that three-dimensional memory chips will become available in the near term.

The development of these stack chips will be driven by other industries (e.g., telecommunications), and use in the nuclear industry would likely occur after they are well established for other applications. Thus, the potential impact on nuclear power applications would be similar to recent evolutionary improvements in IC technology. For safety-related applications, the main issues to be considered for new stacked processors and memory devices would probably be their overall reliability and their environmental compatibility if implemented in other than controlled environments. Thus, the evolution of this technology should be monitored over the long term.

2.3.5 Nanotriodes

Another trend in the IC horizon is the nanotriode. This reinvention of the vacuum tube may show promise for high radiation environments and high temperature environments. The flow of electrons occurs in a vacuum, which should be unaffected by radiation bombardment. This technology is in its infancy but could show promise over the next several years. Progress in development of nanotriodes should be followed over the long term given the potential that this technology could enable smart sensors to migrate into the most inhospitable areas within the reactor containment.

2.3.6 Microelectromechanical systems

Microelectromechanical systems (MEMS), commonly known as micromachines, have a combination of mechanical and electrical features in a very small package. Because of their extremely small size, the mechanical systems are capable of faster, more precise, and more reliable operation than their larger mechanical counterparts. The micron-sized mechanical systems are created by a process called micromachining. This process uses essentially the same steps in the fabrication of an IC and thus allows a two- or three-dimensional mechanical system to be created in the same area that a typical IC would use.

Micromachine technology has been demonstrated in research and development facilities for at least 25 years and, in one form or another, has been in production for about 20 years. Considerable advances have been made in techniques to enable formation of surface structures and iterative etching. MEMS applications include sensors (e.g., pressure, chemicals, vibration), telecommunications (as optical switches) and microswitches. One common application is as accelerometers in air bags. A recent example of MEMS technology applied to contaminant sensing is the "nose-on-a-chip" developed by ORNL (see Fig. 2.10). This MEMS sensor uses microcantilever arrays along a small silicon chip containing electronic signal processing and transmission capabilities. The nose-on-a-chip can simultaneously sense various combinations of hydrogen, nitric oxide, mercury vapor, and alkane thiols in the air.

MEMS technology bundled in a SoC package shows promise for eventual use in nuclear power plants for sensing applications (e.g., add-on vibration monitors, environmental monitors). The long-term progress in realizing this technology for more general applications should be followed.



Figure 2.10. The MEMS application “nose on a chip” uses microcantilevers coated with different chemicals to detect multiple gases.

2.3.7 Molecular Electronics

An emerging technology of considerable interest in the academic community involves molecular-scale electronics, which is a field emerging around the premise that it is possible to build individual molecules that can perform functions identical or analogous to those of the transistors, diodes, conductors, and other components of microcircuits. The primary focus of research is to develop the fundamental components necessary to enable quantum computing. Researchers have developed an electronic switch consisting of a layer of several million molecules of an organic substance called rotaxane. By linking several of these switches together, the researchers produced a rudimentary version of an AND gate. In addition, researchers demonstrated a molecular memory cell. Such memory uses the molecular quantum state to represent a superposition of many stored numbers at once. Because of this multiple-value memory, a quantum computer can theoretically perform several reversible operations on all the stored values in a cell simultaneously. Thus, quantum computing has the potential to revolutionize computing technology by greatly increasing computational speed while significantly reducing the size of the electronics. Recently, it was determined that an ordinary liquid could perform all the steps in a quantum computation, and the nuclear magnetic resonance techniques could manipulate quantum information. However, numerous challenges remain to be overcome before a molecular device that operates analogously to a transistor is feasible. Therefore, although the technology is interesting, it is not likely to develop to the point that it would migrate into nuclear applications within the foreseeable future.

2.4 Computational Platforms

The state-of-the-art for computational platforms lies in the field of supercomputing, but that is of little relevance to nuclear power or process industries. Therefore, the survey in this technology

focus area is limited to selected highlights regarding platforms and system software that are targeted for business and industrial application.

Computational platforms (i.e., the computer systems that host the applications software configured to accomplish specific functions such as control, monitoring, diagnostics, data management, or display) include the following categories:

- workstations,
- desktop computers,
- programmable logic controllers,
- application-specific integrated circuits, and
- field programmable gate arrays.

Smart sensors and the embedded microcontrollers in other equipment could be included, but those are covered in previous sections. Personal digital assistants and other compact or wearable computational devices are likely to see increased use as portable information sources and data storage tools, especially for maintenance and inspection activities in power and industrial plants. However, these are not likely to be used for safety-related activities, so they are not covered within this review.

The nuclear industry is making increasing use of computational platforms for accomplishing a variety of functions, ranging from information access and storage (e.g., plant computers) to I&C systems interfaces (e.g., operations, maintenance, and engineering workstations) to automatic control (e.g., feedwater and turbine control) to reactor protection (i.e., Foxboro's Spec 200 Micro™ and Westinghouse's Eagle 21™). Numerous control system platforms are available for I&C upgrades in existing nuclear plants or foundational I&C systems for near-term deployment of future nuclear plants. Examples include Invensys' Intelligent Automation Series™ (Foxboro microprocessor-based) and TRICON™ (Triconix PLC-based), Framatome Advanced Nuclear Power's (ANP's) Control STAR™ (microprocessor-based) and TELEPERM™ (PLC-based), and Westinghouse's Advant™ (PLC-based) and Ovation™ (microprocessor-based). Four prominent digital platforms are being marketed for safety-system applications:

- Advant AC-160™ from Westinghouse (developed by Combustion Engineering),
- Safety STAR™ from Framatome ANP (developed by Babcock and Wilcox),
- TELEPERM XS™ from Framatome ANP (developed by Siemens), and
- TRICON V₉™ from Invensys (developed by Triconex),

A significant trend exists in the I&C marketplace toward PLC-based systems. To facilitate the use of commercially available systems, EPRI established guidelines⁴⁶ for dedicating PLC platforms for safety-related nuclear power applications. As noted previously, some PLC-based safety systems have been reviewed by NRC. Because of the expanding experience with many of the computational platforms mentioned above, the survey in this technology focus area was directed toward emerging technologies that are likely to increase in use in the nuclear industry or may require development of a deeper understanding of their safety characteristics. Thus, this section presents information on one unique platform that has recently come to the nuclear market and on the more general topic of real-time operating systems, which provide the underlying computing support services for many safety-related applications.

2.4.1 Application-Specific Integrated Circuits

An ASIC is an integrated circuit specifically designed to perform a particular function by defining the interconnection of basic circuit building blocks (e.g., gate arrays, flip-flops, adders, counters, registers). ASICs have been used as hardware elements in many embedded systems. The number of operational states that an ASIC can assume is generally significantly less than for general-purpose microprocessors, and the ASIC can be designed for testability. The design-for-test concept promotes confirmation of the reliability characteristics of ASICs and indicates their potential value as computational platforms for safety system applications. In recognition of those favorable characteristics, a limited number of ASICs that were specifically designed for nuclear power safety applications have been introduced recently.

In the mid-1990s, as part of a Cooperative Research and Development Agreement between DOE and EPRI, an ASIC-based implementation for reactor protection was developed. EPRI, the Westinghouse Owners' Group, and Westinghouse commercialized that technology by the end of the 1990s (see Fig. 2.11). This product is now available as 7300 System ASIC-based replacement modules from Westinghouse. Additionally, Toshiba has recently developed an ASIC-based digital trip module for reactor protection system upgrades.

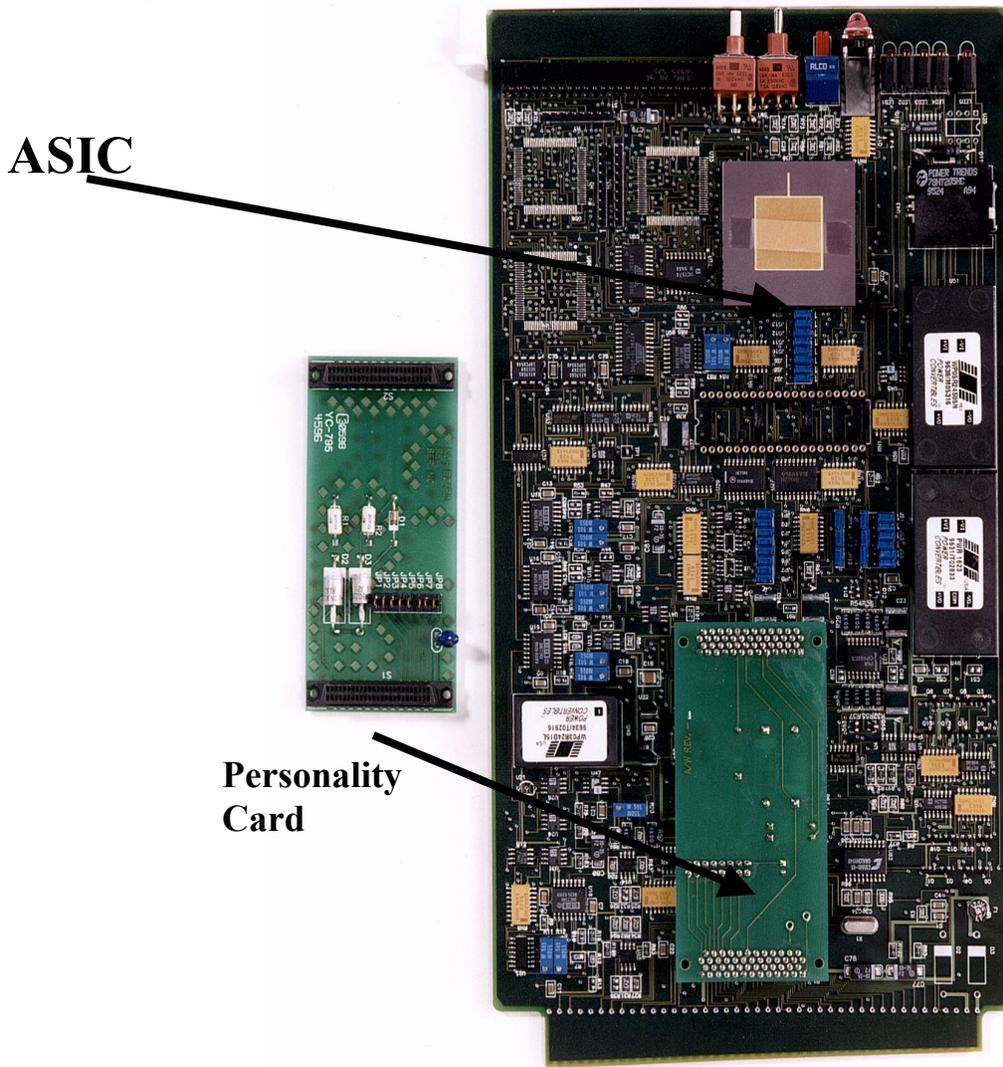


Figure 2.11. Universal ASIC modules can directly replace analog cards in nuclear protection systems.

In light of the potential costs for dedicating commercial software-based systems, it is possible that development of ASIC-based components for nuclear power safety applications will expand in the long term. Therefore, maintaining an awareness of the technology is warranted.

2.4.2 Real-Time Operating Systems

The term *operating system* does not have a precise meaning. Generally speaking, an operating system is a software layer that

- controls the computer and manages its resources, and
- provides a limited interface between application software and operating system services.

The operating system proper might access the computer hardware directly, or it might access the hardware through a lower layer that hides computer hardware details. Some operating systems will use the computer's basic input output system (BIOS) instead of dealing with hardware directly; some operating systems will deal with hardware through a hardware abstraction layer (HAL). The BIOS and HAL are often considered part of the operating system.

An operating system is said to be “real-time” if it provides some mechanisms to give predictability to task execution times. Soft real-time operating systems meet timing requirements most of the time but are allowed to occasionally miss deadlines. Hard real-time operating systems provide the facilities necessary to meet timing requirements under worst-case conditions. This is clearly the most desirable performance characteristic for safety systems.

Advances in computer hardware and ubiquitous computer applications have spurred research into hard real-time operating systems. Small computer systems are increasingly used for smart appliances that gather information and control other devices (see Fig. 2.12). These might be found in industrial instrumentation, video surveillance systems, network controllers, and other embedded microcontrollers. Recognizing these trends, the NRC recently conducted a survey of operating systems and their safety-significant characteristics.⁴⁷ This report describes some of the more significant of those findings.

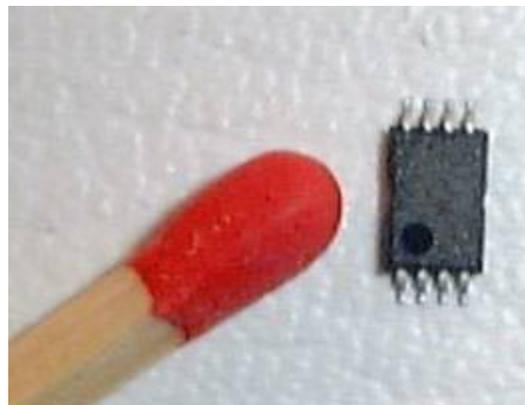


Figure 2.12. This Fairchild ACE 1101MT8 chip implements a restricted, special-purpose TCP/IP stack. Nevertheless, it can serve up real live (if simple) web pages.⁴⁸

Efforts to standardize real-time operating systems include POSIX 1003.1b⁴⁹ and OSEK⁵⁰ (i.e., the European automotive industry specification of conceptual requirements). Beyond standardization, an effort is being made to further define the requirements of hard real-time systems. An extension

of the OSEK operating system, called OSEKtime, is under development and is designed to provide the following characteristics:

- predictability (deterministic, *a priori* known behavior even under defined peak load and fault conditions),
- clear, modular concept as a basis for certification,
- dependability (reliable operation through fault detection and fault tolerance), and
- support for modular development and integration without side effects (composability).

While designed for automotive applications, it is evident that the OSEKtime system meets many of the desired characteristics for safety-related operating systems.

Linux is an open-source operating system adapted by Linus Torvalds from an earlier time-share system called Multics.⁵¹ Today, Linux enjoys widespread support by both university student programmers (because its source code is available for free) and commercial software application developers (including IBM). In March 2002, TimeSys⁵² announced that its Linux products have been optimized to support Sun Microsystem's processors, adding to its list of supported microprocessor architectures. TimeSys offers real-time version of Linux. Another vendor of real-time Linux is FSMLabs, Inc. (RTLlinux). RedHat⁵³ offers eCos,⁵⁴ an open-source real-time kernel currently better suited than Linux because of its relative program size (eCos is around 100 kbytes, whereas a scaled-down version of Linux is larger than a megabyte). As open-source, real-time operating systems become more widely used, research on the advantages and limitations of these systems may become necessary.

Requirements for nuclear safety systems generally exceed those for other industries. In particular, reliability must be very high. This is achieved through redundancy, diversity of hardware and software, and fault handling. Also, the applications using the operating system should be safe in the sense that they cannot defeat the operating system's protection mechanisms. These characteristics are achieved by considering the reliability requirement at every phase of system design. Since most operating system developers focus on the wider market of less-demanding commercial and industrial applications, it is important that nuclear safety concerns have advocates in standards bodies and research groups. Therefore, participation by the NRC in software standards activities would prove beneficial. In addition, near-term research into the performance and reliability characteristics of real-time operating systems is suggested.

2.5 Surveillance, Diagnostics, and Prognostics

Surveillance (i.e., monitoring of the condition of a process or component) and diagnostics (i.e., analysis of the underlying cause of a detected condition) are well established in the process industry. Prognostics is an emerging discipline in which the estimation of remaining useful life is inferred based on diagnostic information and is then used to schedule maintenance on an as-needed basis. On-line monitoring and predictive maintenance are elements of surveillance, diagnostics and prognostics.

In the nuclear industry, surveillance and diagnostics techniques have been employed for many different applications, such as loose-parts detection, core barrel motion monitoring, rotating machinery condition monitoring, instrument response time measurements, predictive analysis of failures in sensors and sensor lines, and motor current signature analysis. EPRI has a Maintenance Applications Center in North Carolina, a Maintenance and Diagnostic Center in Pennsylvania and an Instrumentation and Controls Center in Tennessee where surveillance, diagnostic, and prognostic techniques are demonstrate on fossil plants and for nuclear plants. In addition, the

NERI and NEER programs have sparked additional research in the development of more nuclear applications. Plant life extension, coupled with the economic incentives to extend surveillance intervals and reduce periodic maintenance demands, makes this technology focus area particularly fertile for new applications in current and near-term deployment nuclear plants.

In this technology focus area, as with the others, this report does not give an exhaustive list of all existing techniques and their underlying mathematical basis. Because of the number of previous applications of surveillance and diagnostics, the approach taken for surveillance, diagnostics, and prognostics is to characterize the categories of methods, give some examples of their general application, and then describe current developments related to the nuclear power applications.

Surveillance, diagnostics, and prognostics can be expected to assume an even more prominent role in future nuclear power plants, given the goals of minimizing the operations and maintenance staff, extending operational cycles (thus, increasing maintenance intervals, and implementing multi-modular plants. The integration of diagnostics and controls for autonomous, intelligent plant control and information systems and the transition to greater decision-making responsibility for the machine (i.e., the plant I&C systems) suggest the need for a well-founded understanding of the value added by diagnostic techniques and the reliability of such methods. In addition, greater reliance on prognostics will prompt movement away from periodic manual tests and inspection. Therefore, it would seem reasonable to conduct research on expected near-term nuclear power applications of this emerging technology (e.g., the techniques that are being developed under NERI and NEER) and to monitor development in the technology through awareness of applications in other industries. In particular, methods for assessing the accuracy, stability, and reliability of diagnostic and prognostic techniques are appropriate candidates for near-term research.

Emerging techniques in system diagnostics can be broadly divided into two categories: model-based techniques and data-driven techniques. Model-based techniques use a system model to estimate immeasurable system variables based on currently measured features. The model is usually based on the fundamental physical principles underlying the system. Such techniques require a very high degree of understanding of the system and may provide the user with accurate estimates of system features. These techniques may also be used for system prognostics. The disadvantage of these techniques is that their diagnostic ability is only as good as the system model used in their development.

Data-driven techniques use measured features extracted from historical data (i.e., “training sets”) for various known system conditions to determine the system’s current state. Data-driven techniques are more commonly used than model-based techniques. These techniques require less knowledge of the system but may require extensive “learning” periods to catalog the conditions of interest. They have the additional disadvantage of sometimes giving unpredictable results when presented with system states not adequately represented in the historical data. For example, a diagnostic application based on an artificial neural network may give a credible, but incorrect, result when presented with conditions outside of the training set used in its development.

The application of both types of techniques has become more practical as the price of computational power has decreased. Computationally intensive applications with complex first-principle models of process dynamics, such as reactor physics, heat transfer, and fluid dynamics for nuclear plant dynamic behavior, can now be performed for real-world problems on desktop computers. Thus, more sophisticated model-based system diagnostics have become a practical alternative to traditional diagnostic approaches such as simple vibration monitoring. Similarly, the advanced signal processing and pattern recognition algorithms typically used for data-driven

techniques can be performed for the large data sets typically encountered in applications using desktop computers. It should be noted that approaches described here can be applied at several levels within a facility (i.e., at the component, subsystem, system, and plant level).

One caution should be mentioned, most predictive modeling techniques have an inherent weakness in that they may give unstable or inconsistent results when the parameters used as inputs to the predictor are highly correlated. The difficulties encountered when constructing prediction models with correlated data is not constrained to models based on linear regression techniques. Even greater instabilities can occur in nonlinear techniques, such as neural networks. Additional research and development is needed to assure the accuracy, stability, and repeatability of predictive models used for diagnostics and control. Assessment of diagnostic techniques should include an understanding of the limitations of the methods employed to permit a critical determination of the value of the diagnostic results.

Economic analysis of maintenance actions is an additional dimension that can be added to either model-based or data-driven applications. Given the system state and the cost of various maintenance options, economic analysis can provide information that allows maintenance decisions to be made based on economic parameters such as investment protection, plant availability, or the ability to complete an order by a given date.

2.5.1 Model-Based Techniques

Examples of model-based diagnostic applications include mechanical system identification and process system diagnostics and control. Mechanical system identification uses vibration measurements and a system model to assign stiffness and damping values to system components. By tracking the values of the estimated system component values over time, mechanical degradation can be both detected and located, making maintenance decisions more effective. Such a system has been demonstrated at the Oak Ridge National Laboratory.⁵⁵

An emerging approach is the use of process system models in system diagnostics and control. In these applications, the predicted values of system variables obtained from process system model are compared with measured variables, and the result is used to infer product or process properties or make control decisions. The models used in these applications can be very elaborate, depending on the complexity of the process system, and must be thoroughly verified before being used in the plant. An example of a model-based predictive system is TEMPO, a system to analyze and monitor reactor thermal performance.⁵⁶

2.5.2 Data-Driven Techniques

Examples of data-driven diagnostic applications include signature identification and crack or flaw detection in metal products. Signature identification is the extraction of one or more features from current data that have a strong correlation with the system state. The features may or may not be linked to actual physical parameters. Characteristic signatures may be present in electrical, acoustic, and/or vibration measurements. One approach to identifying the system state involves transforming the time series data into the continuous wavelet domain using the continuous wavelet transform. The transformed signal can be displayed as an image, allowing a wide variety of image-processing and feature extraction techniques to be applied. Global and local image features are extracted, and a probabilistic model of each system state can be formed from the features. Bayesian probability theory can then be applied to identify which system state is the most likely given the current input data. This approach was used in a speaker identification project at the Oak Ridge National Laboratory.⁵⁷ A similar approach using wavelet filtering is used in the Halden Reactor Project's ALADDIN software to classify reactor transients.^{58 59}

An emerging technique for detecting flaws in metal products uses the transmission and reflection of an ultrasonic pulse to detect the existence of a crack or flaw. An ultrasonic pulse originates at a transmitter and propagates through the medium, which typically is a metal sheet or pipe. The received signal, which is a combination of an attenuated version of the original signal plus various signal components caused by reflections, can be used to detect the presence and location of a crack or flaw. The signal processing required to separate the portion of the signal indicative of a crack usually involves a combination of finite impulse response (FIR) and wavelet filtering. This signal processing increases the signal-to-noise ratio and excludes frequencies and times not directly affected by the crack or flaw. This approach has been used to inspect weld quality of Tailer-welded blanks by the automobile industry.⁶⁰

In each of these cases, the features indicative of a given system state or of a certain flaw type are obtained experimentally; the system state or the presence of a crack or flaw is determined from a probabilistic approach or from a pattern-matching or recognition algorithm.

2.5.2.1 Fault Detection for Field Devices

As part of a NERI project, the University of Tennessee is developing techniques to accomplish fault detection and isolation (FDI) of sensors and field devices. The techniques developed for this application are data-driven system models using group method of data handling (GMDH), principal component analysis (PCA) and adaptive network-based fuzzy inference system (ANFIS). The detection of sensor or actuator faults is performed by tracking the model residuals of selected process variables and control functions. Fault isolation is then performed using a rule-based technique and/or a pattern classification technique. Both single- and multiple-fault cases for a test loop and for a simulated steam generator have been considered. An example of detecting the fault in a narrow range (NR) steam generator level sensor is illustrated in Fig. 2.13. The residual directional features (i.e., sensor fault features) are plotted for six different measurements at nine operating levels. The fault feature for the NR level sensor dominates the other feature in this feedback control loop. The FDI system under development is a proof-of-principle demonstration of a key element for an autonomous, intelligent process-control strategy targeted for nuclear power plants.

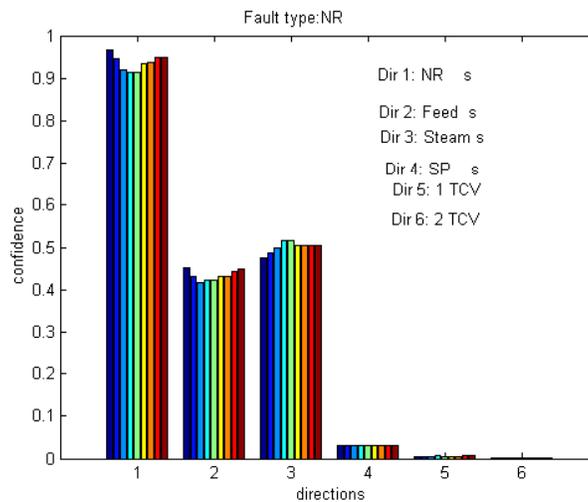


Figure 2.13. Narrow range steam generator water level sensor bias fault for the case of steady-state plant operation.

2.5.2.2 Forewarning of Failure in Critical Equipment

An on-going NERI project at ORNL involves development of a prognostic technique to provide forewarning of failure in critical equipment at future nuclear power plants. The goal of this technique is to reliably detect a condition change and/or forewarn of failure in critical next-generation machinery (e.g., turbines, pumps, and valves). The technique is based on nonlinear analysis of operational equipment data. The research approach is to quantify the (nonstationary) condition change in test equipment as a sequence of robust nonlinear statistical signatures for progression of a fault in specific test equipment. The signatures are obtained for select equipment based on seeded faults. Thus, the equipment response, as evidenced by the signatures, can be related directly to specific fault conditions. The computational methodology being developed first removes irrelevant artifacts from the time-serial data (e.g., periodic variations in three-phase motor power). Subsequent analysis converts this artifact-filtered signal into a geometric (phase space) representation, which in turn is transformed to a statistical distribution function. The underlying assumption is that the complex machine dynamics evolve over a bounded, finite-dimensional region of the phase space. Thus, the distribution function captures a statistical representation of the essential features of process dynamics. Next, information is extracted about condition change, possibly forewarning of an impending failure, via new nonlinear measures that have discriminating power much superior to traditional measures. This technique, coupled with next-generation “smart equipment” (which can be expected to include embedded sensors), will facilitate just-in-time maintenance to improve plant efficiency and eliminate potential safety faults.

2.5.3 Combined Techniques

2.5.3.1 Self-Diagnostic Monitoring System for Balance-of-Plant Components

A NERI project currently being performed at Pacific Northwest National Laboratory (PNNL) involves diagnostics and prognostics of balance-of-plant components. This proof-of-concept demonstration provides the integration of software architecture, distributed and centralized data processing, and smart wireless sensor modules. The approach used in this project is general in nature and should be applicable to monitoring not only balance-of-plant components but also primary system components of nuclear plants.

The diagnostics and prognostics examined in the self-diagnostic monitoring system (SDMS) are based on a combination of data-based and model-based methods. The SDMS focuses on measurement and correlation of basic stressors rather than on the direct measurement of process degradation. The correlation of stressors with process and/or component degradation is clearly data-based. These correlations are used to identify root causes of observed degradation. Prognostics for the monitored components are based on first-principles models.

A considerable amount of data processing is performed by the intelligent sensors, which communicate with a central processing unit using a wireless link. This approach minimizes the amount of data being transmitted by the sensors.

2.5.3.2 Structural and Process Fault Diagnostics for Steam Generators and Heat Exchangers

Under NEER funding, the University of Tennessee is conducting research toward the integration of new, innovative, and existing technologies to develop an automated structural and process fault diagnostics and characterization system for nuclear plant heat exchangers and steam generators. The concept involves model-based and data-driven diagnostic techniques to monitor process degradations (e.g., heat transfer changes due to fouling and deposits) and structural integrity (e.g.,

tubing defects resulting from wear and fretting or stress corrosion cracking and intergranular attack). One technique under development involves characterizing normal and defective tubing based on differences in vibration-induced elastic wave propagation. The research approach consists of devising simulation models to facilitate process degradation monitoring, developing a sensor suite using piezo-electric devices for monitoring structural integrity of steam generator and heat exchanger tubing, and demonstrating *e-monitoring* based on a smart monitoring module (i.e., wireless transmission of data from a smart sensor suite). The models applied in this project include a dynamic model of a U-tube steam generator (UTSG) to simulate changes in its heat transfer characteristics and hybrid physics and data-based models of a typical counter-flow heat exchanger for tuning process dynamics. The goal of the project is to establish the foundation needed for continuous on-line monitoring of structural integrity and incipient fault detection and isolation for steam generators and heat exchangers in nuclear power plants.

2.5.4 Vision-Based Diagnostics

Machine vision technology is another rapidly growing technology in the field of diagnostics and surveillance. Machine vision technology has advanced far beyond the realm of video surveillance, in which a local monitor provides a video image captured by remote camera. Machine vision technology refers to the automated interpretation of digital scenes using computer-based algorithms. The scenes can be generated by a wide variety of imaging sensors, including traditional video, high-resolution, charge-coupled device (CCD) cameras, infrared cameras, and X-ray sensors. Machine vision technology has been widely applied in many industries for product inspection and quality control purposes. In many cases, it provides a methodology for monitoring both the manufacturing process and the resulting product. As the technology base for machine vision continues to grow rapidly, it is destined to become an integral part of diagnostic and surveillance systems of the future.

An example application of machine vision technology with potential use in nuclear plants is monitoring of pumps, piping, and heat exchanger systems using infrared imaging equipment to quickly locate small obstructions in the flow. Another area where machine vision technology has potential application is in personnel tracking and access monitoring. Future machine vision systems will allow automatic tracking, identifying, and logging of all personnel entering and leaving restricted-access areas.

2.6 Control and Decision

The operation of a system or process is managed through the interaction of humans or equipment with field devices (i.e., actuators) that can affect the process (i.e., control). The command for a specific action is initiated by either manual input or automatic control action (or some combination of both) based on information about the state of the system or process (e.g., measurements, diagnostics, constraints, procedures). For automatic control, the command or control action is the result of calculations that are based on process measurements and accomplished by control algorithms implemented in hardware or software. For automatic control, no operator intervention is required, although the automatic control function can be switched out to permit manual control.

In traditional control systems, the decision making (i.e., the choice among valid solutions or options) is left to the human. Elements of the decision process, either during design or operation, include determination of the control strategy (i.e., goals, key variables, available actuators) to be employed, establishment of the acceptable range of actions, and the coordination among individual control loops. In contrast to automatic control, autonomous control involves the combination of control and decision capabilities without required human intervention.

The range of control and decision capabilities constitute the subject of this technology focus area. Control theory is a significant discipline in and of itself. The approach taken in this section for the presentation of survey findings is to group the information by control and/or decision techniques rather than by specific applications. Examples illustrating the use of most of the control techniques described are given, and significant applications and research areas for the nuclear industry are identified.

In the nuclear power industry, single-input, single-output classical control has been the primary means of automating individual control loops. The use of multivariate control, such as three-element controllers for steam generators, has been employed in some cases. In a few cases [most notably the integrated control system (ICS) for Babcock and Wilcox (B&W) PWRs], effort were made to coordinate the action of individual control loops based on an overall control goal. In the 1980s and 1990s, more integration of control loops as part of distributed control systems was accomplished, such as for the digital feedwater control system demonstration project sponsored by EPRI.

The application of other techniques to nuclear power control issues has primarily been the domain of universities and national laboratories (e.g., the DOE Advanced Controls Program at ORNL in the late 1980s and early 1990s). Numerous examples of research into advanced control applications to nuclear power control are reported in the literature. Some of the techniques employed in controls research for both power and research reactors include adaptive robust control for the Experimental Breeder Reactor II, fuzzy control, H-infinity control and genetic algorithm-based control for steam generators, neural network control for power distribution in a reactor core, supervisory control for multi-modular advanced liquid-metal reactor (ALMR). A useful compendium of findings from such research activities is given in the proceedings of a series of Topical Meetings on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies sponsored by the American Nuclear Society.^{61 62 63} Current control systems marketed for the nuclear power industry are based on microprocessors or PLCs. Most of these systems offer control application building software that contains basic control blocks that can be graphically configured into a control algorithm. These systems offer classical control modules as well as model-based control options. Several nuclear power plants have initiated control system upgrades as part of the plant life extension effort. Duke Power's Oconee Nuclear Power Plant in South Carolina recently installed a triple modular redundant replacement of the ICS using the Framatome ANP Control STAR™ modules.

Control systems at nuclear power plants include safety-related and nonsafety, but not safety, applications; therefore, the review of plant control systems as part of the licensing basis has not been as detailed in practice as that of safety systems (i.e., reactor protection and engineered safety features). The primary goal of such reviews is to ensure that the control systems do not introduce operational modes (resulting from design or failure) that can unduly challenge or compromise the safety system function. Therefore, rather than develop research suggestions for each specific control approach, this report offers general observations about control and decision.

NRC has significant experience reviewing control systems based on classical control techniques. Much less (or, in some cases, no) experience exists with the so-called "advanced" control techniques. However, it does not seem necessary or cost effective for each and every method to be researched to assess its performance and reliability characteristics. Instead, it seems sufficient for a general knowledge to be maintained by following long-term developments in the investigation and application of control and decision techniques (primarily carried out by universities and national laboratories or by other industries such as fossil power).

The most significant change that is expected in control system development for nuclear power may be the transfer of more and more of the decision-making responsibility to the I&C systems. Given the staffing and operational cycle goals of long-term deployment reactor concepts and the prospect of multi-modular plants with integrated process systems and/or control rooms, the move to highly automated control and information systems seems inevitable. The role of the human in nuclear plant operations (anticipating the evolution from operator to supervisor with most decisions made by the machine) and the capabilities and reliability of autonomous control systems should both continue to be considered.

2.6.1 Continuous Control Methods

Continuous systems, which are characterized by differential or partial differential equations, are controlled through feedback from proportionally measuring sensors to achieve an output set-point value. Continuous feedback control is a simple automation because the output value is automatically maintained to a set point without constant human intervention. As an example, maintaining core outlet temperature to a specific set point is a continuous control task. The greatest body of control theory literature and tools has been developed for continuous system control. Several control methods and approaches are discussed in this section.

2.6.1.1 Classical Control

Classical or proportional-integral-derivative (PID) control compares the output of a process with a set point to generate an error signal from which an actuator signal is produced to control the process. The method may be used in combination with feedback and feed-forward configurations. Part of the error signal may be augmented by mathematical derivative or integral action to improve performance. PID is almost always used in single input, single output (SISO) control; that is, a single sensor sends a signal to a controller, resulting in action on a single actuator. This form of control works well in many processes. However, performance and stability suffer for processes that are inherently multivariable or nonlinear or that exhibit large parameter swings or structural changes.

In the 1990s, the B&W Owner's Group developed a digital replacement to the original ICS called the plant control system (PCS), which was to be implemented on triple-modular, redundant, microprocessor-based controllers. The PCS coordinates control of the reactor, feedwater system, and steam system. The control system design contains many advanced features to add expanded capability beyond the features of the ICS. It uses digital switching logic to reconfigure the control system to match the plant as valves are sequenced and pumps are started. The PCS control strategy is based on the feedforward-feedback approach. The feedforward input is a centrally generated core thermal power demand. Proportional and integral feedback actions add stability. The following are additional features of the PCS:

- Full automatic control from 1% to 100% of full power;
- Prioritized control of system parameters to maintain control of the most important parameters despite saturation of some actuators or manual control switching for some actuators;
- Automatic loading and unloading of the main turbine and the turbine-driven feedwater pumps;
- Elimination of windup problems in the integral functions of the controller to provide bumpless transfer between automatic and manual control and to improve controller performance; and
- Improved transitions between control modes.

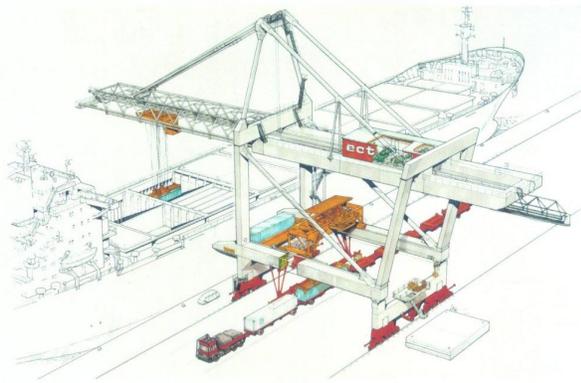
Because of cost considerations, the PCS was never installed at a power plant. However, the PCS became the basis for the revised ICS that was recently installed at Oconee Nuclear Power Plant.

2.6.1.2 Linear Matrix Optimal Control

The linear matrix approach to control, which is based on linear state-space equations, has the benefit of many available mathematical tools for analysis, synthesis, and simulation. One of the tool sets allows the optimization of performance parameters by minimizing or maximizing objective performance criteria (i.e., optimal control). Another tool permits the application of robust methods, which lowers the potential of instability due to noise or uncertainty in plant parameters. Example linear matrix methods include linear quadratic gaussian (LQG), H-infinity, and loop transfer recovery (LQG/LTR). A definite benefit of matrix-based representation is the inherent ability to handle multivariate systems. The weakness, however, with linear methods is the limited dynamic range over which performance is guaranteed. The common approach to design is to linearize the nonlinear system around a nominal operating point, which limits valid operation to a more or less small neighborhood of the operating point. Changes in plant parameters directly influence their performance, which necessitates the need for adaptive control as an adjunct to linear matrix control. In many cases, performance is sacrificed for robustness. Linear matrix methods do not permit easy field adjustment by plant operations personnel compared with classic PID controls because of multivariate inputs and outputs and the complex mathematical gain calculations required.

Examples of state-space optimal and robust control include the following:

- Electro-hydraulic machine tool positioning system for which the response specifications include zero overshoot, zero steady-state error, and minimum rise time;
- Robotic arms and manipulators for industrial assembly and handling systems;
- The Honda Man Robot. Stability is based on state feedback;
- The Segway™ scooter, which has recently been introduced to the marketplace, uses linear multivariate control to achieve balance and stability;
- Rocket engine direction control has relied on multivariate state-space control for decades; and
- Optimal robust controller is being used for jumbo container crane control (see illustration to right).



2.6.1.3 Nonlinear Control

Nonlinear control refers to a wide range of control methods that contain nonlinear factors to compensate for plant dynamics, which contain significant nonlinear response. This topical area is broad and unstructured, unlike linear matrix control. Example topics that pertain to nonlinear control include (1) chaos (theory) control, (2) Lyapunov methods, (3) compensation for deadzone, higher-order effects, and step/jump discontinuities, (4) synchronization, and (5) heterodyning. Stability is not as mathematically simple to predict with nonlinear control compared with linear systems. Simulation is regarded as the ultimate testing method.

Nonlinear control takes many forms owing to the variety of nonlinear systems that must be controlled. Examples include the following:

- Magnetic bearing control (The field does not vary linearly with position and therefore requires compensating dynamics in the control system.);
- Chaos control of burner flame (The chaotic nature of the flame dominates as leaner fuel-to-air ratios are applied.);
- Chaos control of fluidized bed reactors (It has successfully stabilized dynamics over a wide range of operating conditions.);
- Gain scheduling techniques (These are used in high performance aircraft to compensate for wildly varying dynamics over the flight envelope.);
- Phase-locked loops used for communications such as cell phones (This form of nonlinear control is designed to permit phase and frequency lock-in, which is inherently nonlinear.);
- Computed torque and impedance control (This is commonly used by the robotics community to achieve speed of response and stability under varying load conditions.);
- Dynamic inversion methods (Honeywell uses this method for pitch control of an F-14 fighter aircraft and for linearizing valve dynamics in power plant applications); and
- Heterodyning systems (These are used for optical mixing in communications and sensor applications.).

2.6.1.4 Intelligent Control

The methods that are often classified with intelligent control are based on biological and cognitive models of control and behavior. Examples are expert systems, fuzzy systems, and neural networks, which are discussed in this section. (Expert systems are discussed under discrete-event control.)

2.6.1.4.1 Fuzzy Control

Fuzzy logic is a multivalued logic that allows intermediate values to be defined between conventional evaluations such as *yes/no*, *true/false*, *black/white*. Notions like *rather warm* or *pretty cold* can be formulated mathematically and processed by computers. In this way, an attempt is made to apply a more human-like way of thinking in the programming of computers. Values of variables are not restricted to a single set but may have degrees of membership across multiple sets. Ultimately, internal fuzzy variables must be made crisp values to control the outside world. This step is called defuzzification. An example defuzzifier is the *Mamdani* controller, which is based on calculating the centroid of fuzzy outputs. Fuzzy control is suited for very complex processes, when no simple mathematical model or highly nonlinear processes exist and when the processing of (linguistically formulated) expert knowledge is to be performed. Fuzzy control is not recommended if conventional control theory yields a satisfying result, and an easily solvable and adequate mathematical model already exists. Fuzzy logic as a discipline originated in 1965 by Lotfi A. Zadeh, professor for computer science at the University of California in Berkeley.

Fuzzy control has had success in many applications such as the following:

- aircraft fly-by wire control systems;
- automobile engine control systems;

- vehicular traffic control (Ramp metering based on fuzzy logic on the A13 highway in Delft-Zuid is shown here.);
- blood pressure measurement;
- subway control (used in Japan for several years);
- home appliances (incorporated in washing machines for optimal water use in Japan);
- camera-focusing mechanisms for best autofocus;
- temperature control in both commercial building and industrial processes; and
- industrial process control (e.g., rolling mill).



2.6.1.4.2 Neural Network Control

In its simplest form, artificial neural network (ANN) control, which is loosely modeled after human neurons, maps multiple input values to outputs that become signals to actuator devices. At the heart of the network are layers of cross-connections between input and output ports. The weighting values and activation threshold function at each connection determine the function of the network. The mapping (i.e., the weighting values) is learned through a series of training sessions, which may be supervised or unsupervised, and deterministic or stochastic. A network can have feed-forward and feedback connections internally. The function that ANNs perform is distributed across its plexus of connections. This distribution offers tolerance for error and noise at the input. Neural networks are useful for vector functions. Two issues always arise in certain applications: (1) ANNs by their nature cannot be examined to determine their functional properties as one might analyze the gain coefficients of a PID controller and (2) ANNs will always give seemingly plausible results even when operation has been extrapolated beyond the range of all training.

Neural networks have found their way into a variety of control applications:

- elevator control for multiple elevator applications;
- vehicular traffic control—lane control, light control, and speed control; and
- chemical product mixing, especially when the process involves nonlinear dynamics that are difficult to model.

2.6.1.5 Adaptive Control

Direct and indirect model-based controls are used to accomplish adaptive control, in which the control system adjusts to changing characteristics of the controlled plant to maintain satisfactory stability and performance. In all instances some form of plant model is needed to permit adaptation. Model-based control (MBC), which contains dynamic models representing the system being controlled, is based on differential equations derived either from first principles or through system identification techniques. In a direct model-based control scheme, the mathematical model simulates the real process in faster-than-real time. Thus the behavior of a variety of control actions can be simulated and analyzed and an optimum path can be chosen. The direct implementation is prohibitively computer intensive for any sufficiently complex system, and this shortcoming leads to exploration of the use of indirect model-based methods.

The indirect methods use (simplified) mathematical models embedded in the control system to permit adaptation of control gains and coefficients.⁶⁴ One example of using the indirect method

is self-tuning, which has become popular in single-channel PID controllers. A more complex implementation is inverse control, which incorporates an inverse model of the plant or component to be controlled that tames its nonlinearities and dynamics. Convergence becomes an issue in model tuning and adaptation.

Adaptive control methods are very often combined with other control types to permit stable performance over wide ranges and conditions. Common examples include (1) suspension control of vehicles and buildings and (2) acoustic noise cancellation.

2.6.1.6 Genetic Algorithms

Genetic algorithms are used for search and optimization functions making them suited for certain types of control systems. Genetic algorithms are unique systems based on the supposed functioning of living organisms. The method of application differs from classical optimization algorithms in that these algorithms

- use encoding of the parameters, not the parameters themselves;
- work on a population of points, not a unique individual;
- use the only values of the function to optimize, not their derived function or other auxiliary knowledge; and
- use probabilistic transition functions, not determinist ones.

The functioning of such an algorithm does not guarantee success in finding an optimum. In a stochastic system for example, the genetic pool may be too far from the solution. Also, a too rapid convergence may halt the process of evolution. These algorithms are efficient, and are used in fields as diverse as the stock exchange and production scheduling or programming of assembly robots in the automotive industry.⁶⁵

A common control use of the genetic algorithm is in the power factor correction converter for the power industry.

2.6.1.7 Multimode Control

Combinations of differing continuous signal control methods can yield useful results for certain hard-to-control processes. The combinations may range from simple to complex. The ability to simultaneously achieve desired performance and stability is improved by wisely applying several control methodologies. Although specifics depend on the system to be controlled, the overall scheme is to allow several carefully chosen control algorithms (usually based on differing methods, e.g., neural network, linear feedback control, and a model-based algorithm) to process in parallel then choose command signals from one to operate plant actuators. Variations in output command selection include (1) predesignation of specific regimes or conditions over which certain controllers capture control and (2) mixing of all command signals by yet another controller (e.g., fuzzy controller or a command validation algorithm). Permitting adaptation of all the controllers over time enhances the concept.

Sliding mode control, which is a variable structure control, is an often-used form of multimode control. Examples of its use are (1) power controllers and conditioners, (2) hard disk drive control electronics, and (3) robotic and other servomechanisms.

2.6.1.8 Hierarchical Supervisory Control

In most large-scale systems, many processes exist that must coordinate to achieve systemwide performance. Hierarchical supervisory control, whose purpose is to achieve total plant

coordination, permits individual process control by local controllers while exercising top-down coordination across multiple process controllers. The coordination achieves an optimization of materials and energy flow by adjusting local controller set points and other parameters. Coordination also involves switching of controller operational modes (e.g., during maintenance cycles). Automated startup and shutdown as well as systemwide diagnostics are possible with supervisory control. Often hierarchical control involves both continuous and discrete-mode control methods (see hybrid control below).

Hierarchical supervisory control is used to control dams in large river systems. Many bioprocessing systems use hierarchical supervisory control. Another example is DanteII, which was used by NASA to explore volcanic activity on earth.

2.6.2 Discrete Control Methods

Discrete event systems, which are characterized by a finite collection of specific, distinct states and the transitions between them, are controlled by applying logic through combinational and sequential rules. These are not proportional systems (c.f., continuous control). Often, the control of these systems is left to schemes based on heuristic rules inferred from practical plant operation. Industrial plants regularly use PLCs to achieve event control. These commercially available controllers, which are programmed in ladder logic, offer limited intelligence and do not integrate well with complex continuous control algorithms. Start-up sequencing of simple equipment that invokes discrete (binary) steps is well accomplished by PLCs; however, complex machinery, which may have the possibility of multiple start-up paths depending on internal and external conditions, operate beyond the fixed programming of PLCs.

2.6.2.1 Expert Systems

The primary purpose of expert systems is to capture the human capability of diagnosis and control for particularly difficult or specialized tasks. If-then-else rules are the building blocks of expert systems. These rules permit conditional decision making in which the outcome decision is based on the logical condition of input variables. The strategy is to make a rule-based system flexible enough to cope with the many degrees of freedom that arise in large complex systems but manageable enough to design and test. By subdividing the system into smaller subsystems, the development workload can be shared and performed in parallel; nevertheless, the human effort to design large-scale expert systems is large. The logical step taken by developers is to automate the rule building and testing drudgery. Although being done at present, design automation will intensify in the future especially for web-based database systems. Such automation progress will improve economic feasibility for those developing expert systems for large-scale systems.

Expert systems are frequently used in manufacturing and production systems.

2.6.2.1.1 State-based Control

State-based control is a more complex application of if-then-else rules in which the states of the system being controlled are the basis for the structure of the rules. The transition between states is initiated by multiple conditions, which in turn initiate specific actions that drive the system to the desired state. This method may take advantage of graphically oriented display. It is also suited to mathematical formalization. Timing and sequence are handled well with these model types.

State-based control systems are used on batch processes such as those in chemical production plants and manufacturing plants.

2.6.2.1.2 Data-based Control

Data-based control emphasizes internal and external activities. The flow of data and communications is well modeled with this method. However, timing and sequence is not handled as well with this method. State and data control methods may be combined.

2.6.2.2 Intelligent Agent-based Control

Intelligent agent-based control is a growing area of research. Several potential advantages are evident including the “mobility” property: agents can move about in a system to apply their specialty as needed. The literature indicates that intelligent agents have been growing in their use in computer science over the last decade. Intelligent agents have several applications related to control systems: (1) as a carrier and implementer of control algorithms, (2) as a method of communicating adaptation parameters, and (3) as a means of designing the control system both during the original plant design and as a means of upgrading throughout the plant’s lifetime.

Relating to the third application of designing the control system, great possibilities exist for using agent capabilities to capture control system design requirements and create a structure for linking their relationships into a control system. Multiple agents can be assigned to look for and capture according to specific requirement categories. Other agents can scan for inconsistencies and errors as the process evolves. Still other agents can compile resource requirements for the subsequent design steps.

All software agents are programs, but not all programs are agents. The salient differences between traditional computer programs and intelligent agents are compared in Table 2.1. Activities for which intelligent agents offer potential advantages include activities that require teaming and that may cross several computer platforms. Agents are adaptive and autonomous, which may be advantageous for some applications; however, more traditional (static) programming may be appropriate for some precision calculations.

Table 2.1. Comparison of traditional computer programming with intelligent agents

Traditional computer program	Intelligent agent
Static	Dynamic
Direct manipulation—user initiates every action	Indirect manipulation (autonomous)—actions may be initiated by either the user or the agent system
Non-interactive—dialogs are fully scripted	Interacts with user and with other agents
Never changes, unless changed by a human or an error in the program	Adapts, learns
Runs one time, and stops—runs again when called	Persistent—continues to run over time
Predictable—does what it is told to do, even if the command is incorrect	Interprets what is meant, not necessarily the exact command. In the best of circumstances, actions are based on rules, but they may change over time, or in reaction to different circumstances
Follows instructions	May initiate actions as well as respond to instructions
Stays in one place	May be mobile, traveling to other servers

Intelligent agents are beginning to show up in manufacturing systems and interactive robotic systems. The picture to the right is an example of multiagent control for collision avoidance.



2.6.2.3 Non-Mathematical Flow Methods

Multilevel flow models (MFM)⁶⁶ are graphical models of goals and functions of technical systems. Morten Lind invented MFM at the Technical University of Denmark and several new algorithms and implementations have been contributed by the group headed by Jan Eric Larsson at Lund Institute of Technology. MFM has several properties which permit knowledge engineering without mathematical models as used in classical and modern control theory and without rule bases used in standard expert systems. MFM allows diagnostic algorithms to be run in real time without high processor overhead.

2.6.2.4 Formal Methods

Formal methods apply to a broad range of techniques that employ mathematically precise operators to represent states, modes, and actions. The recent emphasis on formal methods has been on automated control system design. An international collaborative effort was mounted in 1996 to apply formal specification methods to generating a steam boiler control system from a specification document. The effort by Abrial et al. produced 33 solution methods from numerous students based on numerous formal languages and constructs.⁶⁷ The conclusion is that there are several viable ways to apply formal methods to capture and design the controller. Since the publication of Abrial's results, others have continued the spirit, making improvements. For example, Petre et al. have examined combining formal and informal design methods to permit better integration with software practice.⁶⁸

Formal methods are more oriented to control system design automation. No commercial product exists as yet.

2.6.2.5 Object-Oriented Control

Object-oriented control takes advantage of information hiding and inheritance properties. The objective is to make the design task less labor intensive, more amenable to analysis and testing, and flexible for modification. For the most part, object-oriented control methods are an extension of object-oriented computer-programming methods (e.g., C++).

Object-oriented control has been used in scientific apparatus and discrete manufacturing systems.

2.6.3 Combined Continuous and Discrete Control Methods

Continuous control systems operating alone experience difficulty achieving their objectives in the face of changing dynamics, such as radical swings in subsystem parameters, component failures, or changes in equipment interconnectivity. In addition, some components are by nature finite state and therefore not controllable by traditional continuous-time methods. Hybrid control is the combination of continuous and discrete-event control to achieve automatic control over a wide range of system conditions, configurations, and desired outputs. At its simplest level, a hybrid controller can be envisioned as a switching mechanism between a collection of continuous controllers. In more complex implementations, the hybrid controller can include a capability to select modes and states of multiple subsystems to effect a coordinated movement to target goals

even with malfunctioning equipment. Diagnostics play an integral role in the advanced hybrid controller to accomplish that capability.

Combining continuous and discrete control techniques often leads to a hierarchical structure with continuous controllers carrying out the tasks of regulation and tracking at lower levels while discrete-event controllers supervise their operation and make more abstract, strategic decisions. For the most part, the continuous parts and discrete-event parts are designed independently and then combined. Discrete-event activities dominate at the coordination and decision-making levels, which exist higher up the hierarchy.

For small-scale systems, the design task of the logic (discrete) component can become complex. The extension to large-scale systems is difficult to scale. A growing body of literature exists for the design of hybrid control systems, most of which to date is applied to intelligent vehicle systems.

Many subsystems contain multiple control types so that discrete and continuous controls must work together at the equipment level. To control a flow loop, for example, may require continuous control of pump speed but also require discrete control over electrical power to motors, oil lift pumps, and valve positioners. (See ORNL/TM-9500 for a more in-depth description of the automation of discrete and continuous control.⁶⁹)

Hybrid control has been applied to direct torque and flux control of induction motors. Other important control applications are automatic piloting of vehicles, induction heaters, power plant boiler control (only experimental at this time), and robotic devices.

2.6.4 Decision-Making Methods

The control of a Generation IV reactor system will probably embody hybrid control and many of the other control types discussed. Diagnostics will be more integrated than they are in current designs to increase autonomous operation and lower operational risk and costs. Diagnostics may execute at several levels: local process, equipment/components, and across multiple processes. The basis for diagnostic decisions may be model based, derived from heuristics (i.e., rule based) or experience (knowledge based), learned over short and long periods (i.e., data driven), or acquired from data mining of other systems. Intelligent agents operating on multiple computer systems, some of which may not be physically at the reactor facility, will accomplish many of these diagnostic activities, therefore making security of those agents an issue to be considered.

An example of the use of decision-making methods for nuclear power applications occurred as part of the DOE Advanced Controls Program. The multi-modular concept for the ALMR involved three power blocks with each block consisting of three reactor systems tied to a common energy conversion system (i.e., balance of plant). The goal was to have one operator per power block. To address the highly complex plant management and reactor system control issues, ORNL developed a hierarchical supervisory control system that integrated controller and diagnostics at the lower levels of the hierarchy with decision algorithms at the higher levels.^{70 71}

2.7 Human-System Interactions

Human factors engineering is treated as a specialized discipline within the I&C field so the survey of this technology focus area has been restricted to selected evolving capabilities or tools of the discipline. Because human-system interactions (HSI) are not identified as a specific topic within the NRC Research Plan on Digital Instrumentation and Control but are treated elsewhere, comprehensive coverage of that technology focus area is beyond the scope of this report. Thus,

only selected highlights are given which represent concepts or systems that are either being developed for specific nuclear power applications or may eventually migrate into the nuclear power industry.

Traditional HSI equipment for plant operations consists of fixed analog displays with some computer-generated trend plotting and processed alarm presentation that have been added over time. Recent upgrades in existing U.S. nuclear power plants have introduced more workstation-based I&C system interfaces using page navigation techniques for information access through video display units (VDUs). Some I&C upgrades have maintained representations of conventional displays through digital mimics of analog devices. Advanced light-water reactor (ALWR) design based its control room configurations on a large-screen display of key plant parameters and collections of operator and supervisor workstations. The N4 plants in France and ABWR plants in Japan incorporate these concepts in their control rooms.

Much research has taken place in approaches for information delineation, operator workload assessment, interaction mechanisms, human reliability assessment, measure of performance, and distribution of control and decision responsibility between human operators and computer systems. NRC is a sponsor and participant for the international research program on man, technology, and organization at the Halden Reactor Project (HRP) in Norway, which has been actively engaged in the application of virtual reality (VR) techniques to control room design. HRP also provides a laboratory testbed, known as HAMMLAB, for demonstration of new control room functions and investigations into human factors issues and repercussions. Key human factors research includes human performance, modernization of control rooms, and virtual reality for design, planning, and safety training. The Man-Machine Interface Systems (MMIS) group at Korea Atomic Energy Research Institute (KAERI) in Taejon, Republic of Korea, also hosts an HSI testbed known as the Functional Test Facility. Finally, under the Nuclear Energy Plant Optimization (NEPO) program, DOE and EPRI have established a working group to draft guidelines for HSI in hybrid control rooms (i.e., existing control rooms that have some digital system interfaces in combination with original analog system interfaces).

2.7.1 Gaze-Contingent Control and Human-System Interaction with Eye-Tracking Systems

The gaze direction and location of the human eye to a calibrated display can be estimated in real-time using a video camera, frame grabber, and software/hardware capable of finding the face, eyeball, pupil and other significant features. The potential benefit of this technology is that it can serve as an input medium for computer control instead of command language or peripheral control (e.g., a mouse, trackball, touch screen). This is an extremely rapid and natural form of computer communication that could be quite useful to an operator at a workstation under peak workload conditions. Gaze contingent control can be used to navigate a complex three-dimensional (3D) graphical environment, provide information about graphical objects in the scene, select menus, or perform any number of human-system interactions. In addition, gaze-aware intelligent agent software could use this information to update a temporal model of user attention and prompt the user about needed areas of attention. The best eye-tracking systems are nonobtrusive and noncontact, fulfilling an essential condition for user acceptance. Some of the newer systems also do not require infrared or other light-emitting devices.

Eye-tracking is already an integrated component of some virtual-world systems. For approximately a decade, LC Technologies, Inc., has offered a completely gaze-controlled computer interface for use by disabled persons. Applied Science Laboratories has a model (ETS-PC II) on the market that tracks eye movements in an automobile or simulator under virtually any lighting condition. Thomas Schnell at the University of Iowa developed a demonstration prototype of a system that uses eye movements as an alternate method of control activation in an

aircraft cockpit. The military aviation community is very interested in this technology, but it is also being explored in the context of commercial aviation.

Although eye-tracking technology is in some respects quite mature, some issues persist that limit the scope of application to complex real-time environments. Robust and reliable head tracking has still not been well integrated with eye-tracking technology. Consequently, it is necessary for users to limit head movements within a small space. This condition is perhaps acceptable if user space is restricted to a cockpit or driver's seat, but free ranging motion in a control room environment would need to be accommodated. Accuracy and calibration, especially in the peripheral range, and the need to recalibrate are other research issues that remain to be resolved before the technology can be brought into general field use. However, as an alternate method of human-system interaction or control activation, the technology may be ready for near-term deployment. The technology could be moderately useful to an operator in the nuclear power plant control room under information-rich peak workload conditions where quick response is required. Eye-tracking will likely be a standard interface option (much like speech recognition) for the advanced workstation of the future.

Because of the technical issues that remain, long-term monitoring of this technology and applications to real-time control environments is reasonable. At the same time, it would be useful for the nuclear power research community to perform applied research targeted at specific uses of eye-tracking for control activation and human-system interaction in the control room. Another possible application is head-mounted eye-tracking devices for the maintenance worker equipped with a portable computer or a personal digital assistant. Gaze-controlled heads-up displays outlining written maintenance procedures or diagnostics would free the hands for manual work. Head-mounted eye trackers are a more mature technology because they do not have to factor in head movements to the calculations.

2.7.2 Software Agent-based Operational Support Systems

Agent-based systems have received a great deal of attention in recent years, and can be potentially extremely powerful. Operators/users can delegate to a society of software agents tasks that are either too time-consuming or mundane to perform themselves or that cannot be accomplished by humans in the available time frame.

Many agent-based applications already exist as demonstration prototypes or functioning systems. A generic agent framework called the advanced plant analysis and control system (APACS) was designed to monitor and diagnose real-time nuclear power plant failures. The development of APACS was supported by the Canadian government and undertaken by Ontario Hydro and others. Another agent system, the adaptive intelligent system (AIS), has been implemented to perform process control tasks such as monitoring of hospital patients, materials processing, aircraft control, and tutorial instruction. The reusable environment for task-structured intelligent networked agents (RETSINA) infrastructure has been extended for use in wearable computers for aircraft mechanic decision support during aircraft maintenance. During inspection, the mechanic fills out a computer form when a discrepancy is found. An agent analyzes the form and seeks out relevant information from a society of agents. The system then displays recommendations from the processed information. Advantages of wearable computers with agents include faster retrieval of repair information, better access to historical repair data, greater efficiency in using manuals, and reduction in repair time. The optimal aircraft sequencing using intelligent scheduling (OASIS) is a prototype air-traffic management system that combines artificial intelligence, software agents, and conventional software techniques. OASIS calculates estimated landing times, determines the sequence of aircraft landings to minimize delay, and advises air traffic controllers of appropriate control or corrective actions to achieve this sequence.

Some described agent properties such as autonomy and proactivity raise significant challenges for usability. Research in this area has not sufficiently dealt with issues of human-agent communication from the user’s perspective. Human-system interfaces for complex systems are difficult to design correctly, and interactions with agents possessing considerable power and autonomy creates a great potential for error in complex systems where safety is a significant concern.

Agent technology is not yet mature, and standards are still emerging. Nevertheless, agent systems are already appearing in the nuclear industry (see following sections), and focused research programs would be beneficial to ensure that agents are not introduced into nuclear power plants in haphazard fashion. Initial applications in monitoring, diagnosis, and decision support to operators and maintainers are the most likely areas for the application of agents-based systems as part of near-term deployment. Automatic control of power plants by agent-based systems is more likely an option for long-term deployment.

2.7.3 Virtual Collaborator

Humans rely on many modes of communication that are not present in computer interfaces. Human vision is 3D and takes advantage of many clues found in 3D vision that show objects’ grouping, size, and distance from the viewer in 3D space. Thus, human abilities in spatial memory and pattern are not fully used in two-dimensional displays. In addition, social communication abilities are generally not used, such as gestures, facial expressions, tone of voice, and emotional content.

Research and development has been on-going in these areas. One such project of relevance to nuclear plant operations imagines a “virtual collaborator” (see Fig. 2.14), which is a human-like software agent inhabiting a virtual reality space and assisting plant operators.⁷²

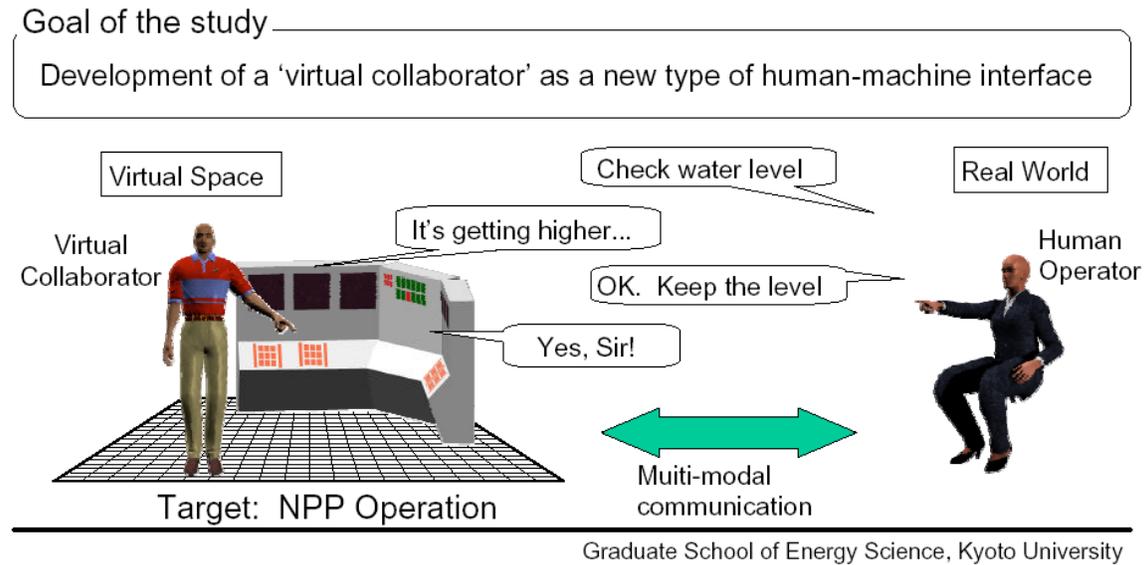


Figure 2.14. Virtual Collaborator—Software-agent-based operator assistant

Ultimately, such an agent-based interface would enable the plant operator to engage in very human-like interaction with the plant systems. This technique would allow the operator to elicit

more complete information about the plant and facilitate learning by intelligent computerized monitoring systems of operator preferences for information presentation and content.

2.7.4 Content-based Information Retrieval

Advances in computer performance, communications, and storage will make it possible to routinely acquire and store complete records of plant operations and maintenance activities. Records could include sensor readings, video records, and documents. While such a complete record may be desirable, it presents an information retrieval problem. One possible solution is content-based retrieval, often applied to image retrieval.^{73,74}

Records are routinely indexed by time and sensor, and are searched by queries based on these values. Often the user needs to search records by querying about the content. An excellent example is the Internet; search engines look mainly for content and only consider date and record location as secondary indices. Because much Internet information is primarily text, information retrieval technology has been developed to search for text content. Currently, web search engines maintain large keyword indices to describe content. The next step is to make web page content more meaningful by adding meta data via XML (eXtensible markup language). This will allow search engines to refine their searches to find not only words, but “words” with the required meaning. Another tool is a program named FERRET, which is a knowledge base retrieval system.

Records in operations data systems at future nuclear plants likely would also contain instrument identifiers and data output. The content indices for such records need to be suited to the nature of the data and type of measurement. For example, a continuous video record of the containment area would contain a wealth of information about the activities inside. A user might be interested in knowing the times that anyone was near a certain instrument. A content-based image retrieval system would search the records and locate those images by its ability to recognize people and the camera location. This technique further allows a very interesting sort of query in which the user presents an image of some person or object to the computer (perhaps a tool has been lost) and asks the computer to locate records with this object. In a similar application, audio records could be searched using technology that already exists for speech recognition.

Another example is a query of plant performance data from instruments. As an example, some plant system may have just experienced an anomaly, leading the user to search for any similar anomalies from the past. In this case, the user could present the instrument readings during the recent anomaly and ask the computer to find similar anomalies, if the appropriate indexing existed.

Finally, a comprehensive system could tie together records from a wide variety of sources (e.g., images, audio, sensors, maintenance records, engineering documents) to gather a complete picture of events of interest.

The use of emerging information management and access technologies is expected to become pervasive in future nuclear power plants. With a goal of minimizing the number of operational and maintenance staff, long-term deployment reactor concepts can be expected to have highly integrated control and information systems facilitated by sophisticated information management and interaction technologies. As a result, emerging techniques and approaches in this field should be monitored over the long-term. Near-term research may be appropriate for specialized applications.

2.7.5 Biometrics

Traditionally biometrics refers to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. The term biometrics has also been used to refer to the emerging technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition. Biometrics is the science of identifying people through biological markers just as reliable as fingerprints, such as voice recognition keyed to highly valued representation systems or quick computerized scans of faces, palms, or the inside of eyeballs, whose detailed features are unmistakable signatures of an individual.

Biometrics are best defined as measurable physiological signature patterns that can be utilized to verify the identity of an individual, which is of increasing importance in the nuclear power plant environment. Biometrics in the nuclear power plants could include surveillance interfaces for detecting identity markers (including hand geometry, voice patterns, facial recognition). These markers would be the basis for verifying identification for security or to automatically customize digital recognition of operator screens for shift changes.

Another area of focus is characterization of individual and groups for reducing internal and external threats. Here the research and application is on characterization of signature patterns to determine thought process in decision-making at a neuro-physiological level coupled with psychological assessments for identifying internal vulnerabilities. One such approach is a Unified Field Theory for Human Behavior Assessment. With the onset of computer network exploitation and attack tools, and the possibility of biological intrusion, a richer understanding is required of our own vulnerabilities within our design of advanced control room operations.

These techniques would probably be of benefit to the nuclear industry because sabotage or terrorism avoidance depends on verification of the true identity of individuals and anticipation of action. Therefore, these techniques should be well understood and their development should be followed.

2.7.6 Automated Visual Surveillance for Facility Monitoring

Automated visual surveillance (AVS) is a composite of several emerging technologies that will probably be employed in the future at restricted sites that are critical to the nation's infrastructure (e.g., nuclear power facilities) in an effort to improve security. An AVS system, which can be coupled with existing security mechanisms, can provide capabilities beyond what is available from traditional security systems. Examples of such advanced capabilities are given below:

- AVS can provide additional safeguards at access control points. One or more video cameras connected to a computer can be used to perform face recognition at access control points. This can improve security personnel performance or, if coupled with additional access controls (e.g., palm or iris scanning, coded badges, or keypads), can be used to replace security personnel at some access points. Furthermore, face recognition at a facility access point provides an initialization for video-based personnel tracking and monitoring within the facility, thus providing a tool for proactively addressing sabotage risks.
- Within the secure areas of the facility, video cameras and robust face recognition can be used to detect, identify, and monitor personnel. Anomalies, such as personnel in unexpected locations, can be detected and send an alert to security personnel.
- Video-based face recognition can be used in conjunction with other personnel tracking mechanisms, such as radio-tagged badges, to enhance security and eliminate potential

pitfalls. With radio-tagged badges, for example, an employee may leave his or her own badge behind or use another employee's badge. An AVS system can detect personnel with video, note the absence or mismatch of a radio tag, and alert the security personnel.

- An AVS system can be used to observe certain critical objects. Relocation or removal of such objects can be used to trigger an alert.

As indicated, a key component of AVS is face recognition. Existing face recognition technology uses information from only a single image, rather than multiple observations from several cameras or a video sequence, and suffers significantly in the presence of compounding factors such as varying illumination, facial expression, decoration (e.g., eyeglasses and/or facial hair), and pose. These deficiencies lead to only a 50-60% success rate for current facial recognition systems. Projected advances in face recognition technology are directed to address such limitations and increase the recognition accuracy.⁷⁵ Other emerging technologies that contribute to AVS include video and image processing,^{76 77} video-based person detection and tracking,^{78 79} and face tracking in video.⁸⁰

The emergence of wireless computer applications raises an issue that needs consideration for surveillance and threat reduction. Application of such technology can enable personnel to access information from anywhere within the facility using a personal digital assistant (PDA) that can download and display critical data via a screen on the PDA or through a mounted eye piece. The system should provide voice feedback recognition and authentication to facilitate remote access of data by trusted users through voice command. Systems exist currently that can achieve the above.

2.7.7 Virtual Reality

Utilization of VR technology has been shown to be a powerful tool in control room design and application research. For example, a VR environment can enhance the ability of an operator to access information that capitalizes upon natural aspects of human perception by extending visual information in three spatial dimensions (e.g., see previous section, "Virtual Collaborator"). In addition, fundamental VR knowledge and methods can be used to develop tools to facilitate design, planning, and training for the nuclear industry (e.g., control room validation, decommissioning planning, and maintenance training), and to provide a mechanism for testing various scenarios for characterizing human behavior as part of vulnerability assessments of information operation applications.

The VR center at HRP is focusing on development in four key research areas: virtual humans (i.e., intelligent manikins, manikin realism, distributed avatars in a networked virtual environment for various kind of training), design and ergonomics (e.g., shared environments, intelligent design methods), performance assessment (i.e., VR test and evaluation) and wireless technology (to support presentation of plant status, enhanced communication, and augmented reality for the use of computers to overlay virtual information). A specific example of practical application of the VR center research involves the efforts of a joint Russian-Norwegian team to reduce human-based errors and dramatically increase operational safety during the refueling process of an RBMK-type reactor. Success was achieved by implementing a training simulator based on an innovative VR approach in which a traditional display-based simulator was extended with VR models of the actual refueling machine and its environment to improve both learning and operational effectiveness.

NRC cognizance of HRP research should prove instrumental in maintaining awareness of the capabilities and prospects of VR applications for nuclear power applications. In addition, the NRC should continue to follow research in VR for other industries.

2.8 High-Integrity Software

The field of high integrity software has been a highly evolutionary one for the past 30 years. As a result of the continuously expanding uses of software in every aspect of life, many highly critical engineered systems have begun using software-based digital systems. These include control of passenger aircraft, many kinds of military hardware addressing diverse functions ranging from ship navigation to targeting of smart bombs, the national electrical grid, and many forms of diagnostic and therapeutic medical devices. Because of the high consequences of failure of these systems, the need for high integrity software has increased significantly. From the perspective of its use in nuclear power plants, the current plan by several utilities to retrofit reactor protection I&C systems with software-based digital systems is leading to the need for new methods for developing and assessing software with very high levels of quality and reliability. The aspects of high integrity software included in the discussion are software development methods, software assessment methods, and software reliability.

The industry requirements for computer-based safety systems are identified in Annex E of IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." IEEE 7-4.3.2 requires that digital safety systems be designed, fabricated, installed, and tested to quality standards commensurate with the importance of the safety functions to be performed. Industry practice involves establishing a software life-cycle process at the beginning of the safety system development. The software developer may be the licensee, the vendor, a company working on behalf of either, or a commercial software development company. Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE 1074, "Standard for Developing Software Life Cycle Processes," provides guidance for the implementation of a software life cycle plan. Developers of software for nuclear applications generally still use traditional software development methods.

2.8.1 State of the Practice for High-Integrity Software

Research and development in the area of high integrity software is being carried out by both industrial and university-based research groups in this country and abroad. As microprocessors have become more powerful and available, the number of software programmers has risen dramatically to meet the needs of users. The ability to write large, complex programs by combining blocks of software written previously by others as well as using object-oriented software development tools has led to a plethora of different software development methods. However, the need in high-integrity software for very high quality and reliability has led to specialization in this area. While the number of general software development houses has increased dramatically, the number of people devoted to high-integrity software has risen less quickly.

Research for the consumer electronics industry has focused primarily on functionality and has not concentrated on software failures. The aviation industry research has led to improvements in software quality but in many instances there is still some reliance on pilot intervention in the case of significant software failures. The telecommunications, fossil power, chemical processing, glass, steel, aluminum, paper products, and metal forming industries, while interested in reducing failure rates, are also continuing to rely on high levels of redundancy and administrative controls. The most significant research in software engineering methods is currently being done in the aerospace, transportation, and military fields. The consequences of software failures for military, aerospace, and transportation applications forced these industries to continue development of ever-increasing levels of quality and reliability for software.

2.8.2 Software Development Technologies, Methodologies, and Tools

Software engineers have tried to improve the quality of the software while at the same time they have been trying to control the costs of the software-driven systems. To satisfy both of these goals, they have developed (and continue to develop) standards for production and assessment of the software throughout the software life cycle. The IEEE has been developing software standards since 1976. The IEEE has published a Software Engineering Standards Collection, most recently in 1999. This collection includes 40 IEEE software engineering standards. The standards cover software life cycle processes, project management, software engineering plans, documentation, reuse, tools, and measurement.

The ISO and the International Electrotechnical Commission (IEC) have led the development of ISO/IEC 12207:1995, “Information technology–Software life cycle processes.” The ISO also has issued ISO 9000-3, “Quality management and quality assurance standards–Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software,” to extend the approach of ISO 9001, “Quality systems–Model for quality assurance in design, development, production, installation and servicing,” to software. The IEEE software engineering standards probably represent the best picture of the overall state of the practice for software engineering.

Along with the standards, software engineers have been developing methodologies and tools for software production and assessment of the end product. One such methodology is the Capability Maturity Model (CMM), developed by the Software Engineering Institute (SEI) at Carnegie Mellon University. This methodology, focused primarily on the process, has been very influential in software development. Work at the SEI has continued beyond the CMM method for assessing software developer capabilities to include two newer methods—the Personal Software Process (PSP) and the Team Software Process (TSP)—that use software measures to help improve the quality of developed software.⁸¹

Some other research centers are providing guidance on methodologies for high quality software that is based on empirical studies. For example, the Center for Empirically Based Software Engineering (CeBASE) has reported guidance on life-cycle selections in which it discusses the suitability of the sequential waterfall model versus the (spiral) evolutionary development model as a function of considerations such as the extent to which the requirements are known and stable, the identification of requirements with high-risk implications, the availability of a known viable architecture for implementing the requirements.⁸²

Other researchers have developed software engineering methods that include explicitly mathematical foundations. These methods include the formal method for assuring specification. This method requires that software specifications be formulated in mathematical relationships so that the final software can be used to “prove” that the specifications have been met. This method has traditionally been very useful in some settings. However, in real-time systems, which are common in nuclear power plant applications, the inability of the method to deal with many aspects of real-time systems, such as timing, has limited its usefulness. Research in this area includes a new formalism called causal functional representation (CFR). CFR allows the specification of conditions that are satisfied by a behavior, such as an occurrence of a temporal sequence of events or causal relations among external events and a system component.

In the early 1980s Harlan Mills of IBM developed the theoretical foundations of the “Cleanroom” process for the production of high-quality software.⁸³ Cleanroom theory is based on mathematical function theory. Cleanroom software engineering is characterized by three principal technologies—incremental development under statistical process control; function-based

specifications, design and verification; and statistical testing. Incremental development is driven by planned development of software in increments with testing against requirements at each increment. Quality of the software is assessed at each increment, and statistical process control is used to ensure the identification of process deviations.

Function-based specifications, design, and verification used in the Cleanroom method employs what is known as the box structure. The specification begins with an external view (called the black box), is transformed into a state machine view (called the state box), and is fully developed into a procedure (called the clear box). This design method permits the use of object-based design (the boxes support information hiding and separation) while it maintains the advantages of detailed verification. Correctness verification is done for each box, based on (1) external requirements for the black box, (2) state data for the state box, and (3) the procedures (paths) through the software for the clear box. Statistical testing is done based on a usage model that represents the population of all possible system states. Testing is treated as a matter of statistical problem solving with test cases generated to maximize information based on the testing time, resources available and the decision to be made. The Cleanroom software engineering method has shown significant successes in high-integrity software applications, particularly for DoD and NASA projects such as satellite control systems.

Software systems are known to suffer from failures caused by transient faults. Recently, the phenomenon of software aging—the state of the software systems degrades with time—has been reported. To counteract this phenomenon, a proactive approach of fault management called software rejuvenation, has been proposed. This essentially involves gracefully terminating an application or a system and restarting it in a clean internal state, while retaining state knowledge (what was happening before the failure). Research is currently exploring the use of measurement-based models that use strategies for software rejuvenation that is triggered by actual state measurements. In theory, the system will sense that it is about to fail and rejuvenate itself prior to failure. Potential exists for this method to be useful in real-time applications.

2.8.3 Software Assessment Methods and Technologies

Several different types of reliability assessment methods are available, including reliability growth models, measurement-based dependability, and stress testing. To date, none has proven to be sufficient alone in proving the reliability of very high quality software. New research in this area is focused on increasing software assessment capabilities.

Some interesting empirical insights are being reported from the CeBASE. According to a recent presentation at the Twenty-Fifth Annual Software Engineering Workshop sponsored by NASA Software Engineering Laboratory (SEL),⁸⁴ “Under specified conditions..., peer reviews are more effective than functional testing for faults of omission and incorrect specification...; functional testing is more effective than reviews for faults concerning numerical approximations and control flow....” Also, Jack Ganssle⁸⁵ (The Ganssle Group) references reports from IBM, HP, and AT&T about the benefits of code reviews. Specifically, double-digit gains in productivity and double-digit reductions in coding errors are reported.

Research by the University of Maryland classified 40 software metrics and ranked them according to their importance to reliability.⁸⁶ (It should be noted that the NRC does not use quantitative reliability goals as the sole indicator of software regulatory compliance.⁸⁷) The more important a software measure is to reliability, the more accurately it may predict reliability of the final product. Because the ranking of each software measure was performed at each stage of the software life cycle, it may be possible to accurately predict the reliability of the final product as it progresses through the various stages of the software life cycle. By combining the highest ranked

software measures into reliability prediction systems (RPS), it may be possible to improve the accuracy of the prediction.

Recently a limited scope validation of this approach was completed.⁸⁸ The results were reviewed by some of the same experts that participated on a panel for NUREG/GR-0019. The experts agreed that further research is warranted, with additional effort required in applying the methodology to a larger, more complex real-time control system as well as using a larger set of software measures (and thus RPSs). One identified shortcoming is the accuracy of the predictions. Whereas a high-integrity system may need reliability to the fifth decimal place, the current capability of the methodology is limited. However, all experts considered the methodology capable of enhancing the assurances of software quality and reliability.

As software reliability increases, failure rates become low and hard to measure. Some researchers have adapted importance sampling to enable the measurement of software and system reliability for high-integrity systems. The technique uses the operational profile and expected exception conditions to create both a testing program and the definition of importance factors. This methodology is reported to allow testing results to be evaluated quantitatively in order to conservatively estimate failure rates lower than 1 per million hours.⁸⁹

Other researchers are using other stratified sampling methods, such as orthogonal defect classification, which have shown promise in accelerating reliability growth models of software reliability. In this method faults are categorized into classes that collectively point to the part of the process that needs attention, much like characterizing a point in a Cartesian system of orthogonal axes by its coordinates. The developmental testing of the software is then concentrated in that area of the defect space that will accelerate the reliability of the software the fastest. As this area becomes less important to systems reliability, the method updates the point and concentrates testing in a new area.

In addition to the use of importance sampling (see above), another view can be taken of high-integrity systems when reliability is very high and relatively little failure data exists on which evaluations can be made. This method involves a qualitative evaluation of the data and the search for trends. This is not a technology so much as a methodology, as extensive experience and insight are required for its success.

For a more quantitative view, we need fairly sophisticated mathematics to understand the level of integrity of software that does not fail during testing or usage. Some researchers are considering the “statistics of rare events” to determine how this branch of mathematics can be used to improve assessment of the reliability of very high reliability software.⁹⁰

Many researchers point out that safety is a systems problem, not just a software problem. They encourage the testing of digital systems in which the software is operating on (or in) the hardware. The Center for Safety-Critical Systems is located at the University of Virginia. This center is a leading research center for testing integrated hardware/software safety-critical systems. Some of the center’s work is in the area of nuclear reactor applications.⁹¹

In addition to the development of new methods, the availability of ever-increasing computational resources may allow for the ability to run much larger numbers of test cases in a reasonable amount of time. For example, the Lenux cluster computer installed at the NRC Office of Nuclear Regulatory Research provides computational power that was available only at the nation’s most powerful supercomputers a few years ago. This capability may change the testing paradigms that

have evolved through years of using much slower machines. This machine and others like it will become available to software engineers to perform software testing in the future.

2.8.4 Object-Oriented Languages: Real-Time Java

In November 2001, a real-time specification for Java (RTSJ) became available.⁹² The RTSJ extends the Java platform to include support for advanced real-time application programming—both hard and soft real time. This extension is compatible with several implementations of Java, including embedded Java and personal Java. Availability of RTSJ fills the need of providing real-time systems with the required strong deterministic guarantees and/or control in the areas of thread scheduling, synchronization overhead, lock queuing order, class initialization, maximum interrupt response latency, and garbage collector (GC) characteristics. These needs were not met by the standard Java platform, and no other extension addresses them.

Although this step is necessary for Java to move into high-integrity real time software development, more work is needed to bring the RTSJ closer to the tool that engineers need for developing embedded system. In particular, a compact version of the real-time Java kernel—small enough to fit on microcontrollers or single-board computers (around 50–100 kbytes)—is needed.⁹³ Because of the extensive and growing use of Java by web and enterprise application developers, real-time embedded Java should be expected to become much more prevalent in the software market over the next few years.

3. PROSPECTIVE EMERGING TECHNOLOGIES RESEARCH TOPICS

The emerging technology survey provides an opportunity to assess recent advancements and expected developments in the I&C discipline. This section presents observations about potential safety-related issues posed by the emerging technologies that were identified in the survey and offers conclusions about those that should be considered for near-term research or warrant monitoring based on their potential for migration into safety-related nuclear applications. As expected, the survey findings confirmed the need for the technology and applications research elements specified in the NRC Research Plan for Digital Instrumentation and Control. The observations and conclusions presented in this section are grouped in terms of the technologies that are addressed by the I&C research plan, the technologies that suggest potential near-term research needs that are not explicitly covered in the I&C research plan, and the technologies that may warrant long-term monitoring of future developments.

The findings, observations, and conclusions from this survey serve as input for the on-going process of refining and enhancing the NRC Research Plan for Digital Instrumentation and Control. The emerging technologies that are identified in areas that correspond to research elements already addressed in the I&C research plan confirm its technical focus and suggest specific topics that may contribute to establishing a detailed research approach to be followed. The near-term research needs for emerging technologies that are identified in areas not directly addressed in the I&C research plan offer supplementary topics that can be considered in subsequent enhancement of the plan. The emerging technologies identified as warranting long-term monitoring provide pointers to technologies that are generally not considered to be sufficiently mature or well demonstrated to impact near-term deployment but which may lead to potential future research needs. Finally, it should be noted that this survey proves a “broad-brush” overview of a significant number of technical topics. It is recommended that periodic surveys be conducted of specific technology focus areas (or subsets thereof) to provide more depth in the identification and assessment of emerging technologies with the potential to impact safety-related I&C applications in nuclear power.

3.1 Emerging Technologies Addressed Within NRC Research Plan for Digital Instrumentation and Control

The NRC Research Plan for Digital Instrumentation and Control contains an element (§3.5.3, “Advanced Instrumentation”) addressing advanced instrumentation in anticipation of technological advances and/or new sensing techniques. The tasks described under this element include the investigation of advanced instrumentation (i.e., sensors) that is expected to be introduced for nuclear power use and the identification of characteristics that either enhance or degrade safety.

In large part because of the research impetus due to NERI, INERI, and NEER, several new instruments are under development that are identified as being potential candidates for eventual implementation in nuclear power plants. Most of the sensor technologies described are in a state of research development or are in the process of demonstrating their capability for nuclear power applications. The clear exception is ultrasonic flowmeters, which are already being marketed and implemented in the nuclear industry and have been evaluated by NRC as key factors in requested power rate increases. However, continued monitoring of experience with the flowmeters and any further developments is suggested.

Of the emerging sensor technologies still under development, silicon carbide neutron flux monitors, which offer the potential to combine the functions of current three-range flux monitoring into a single system, showed the greatest maturity. Therefore, those instruments are

considered to be the most likely new sensor technology for near-term deployment in existing or evolutionary reactors. It is noted that a more detailed understanding of the characteristics and capabilities of silicon carbide neutron flux monitors may prove necessary in the near term, depending on the continued development of the technology.

The remaining new sensor technologies for traditional nuclear and process variable measurement are identified as candidates for long-term monitoring to keep track of their development and anticipate the need for more comprehensive investigations. The emerging technologies include the solid-state neutron flux monitor; fuel mimic power monitor; miniature scintillation-based, in-core, self-powered neutron flux and temperature probe; Johnson noise thermometer; magnetic flowmeter, Fabry-Perot fiber optic temperature sensor; and optical pressure sensors.

Some emerging technologies are related to sensing needs associated with innovative reactor concepts. These are gamma-ray tomographic spectrometry for pellet fuel and core monitoring, and a hydrogen sensor for entrained gas monitoring and facility or process monitoring as part of nuclear-driven hydrogen production. In each case, monitoring the evolution of these technologies is suggested.

The NRC Research Plan for Digital Instrumentation and Control also contains an element (§3.5.4, “Smart Transmitters”) addressing smart sensors or transmitters. Given the potential benefits offered by functional consolidation, self health assessment (e.g., self calibration, heartbeat, onboard diagnostics), and improved information (e.g., signal validation, virtual measurements), it is rightly anticipated that smart sensors will eventually migrate into safety-related applications at nuclear power plants. For those reasons, and because of the market forces that are driving more vendors to intelligent digital product lines, it is observed that this technology should be considered for more thorough investigation in the near term. This is consistent with the I&C Research Plan.

Wireless communications is identified as a research element (§3.5.5, “Wireless Communications”) of the NRC Research Plan for Digital Instrumentation and Control. In this survey, it is observed that the use of wireless systems in the nuclear industry is occurring now and is expected to significantly increase in the near term because of their cost, availability, and flexibility. Given the limited experience with wireless communications for highly reliable, secure data communications, near-term research is needed to better characterize the deployment issues (e.g., reliability, security, and electromagnetic compatibility) that should be addressed to enable safety-related applications of this technology. Based on the rapid pace of advancement and product development for this emerging technology, the recently initiated research project is timely.

Under the topic of firewalls, the NRC Research Plan for Digital Instrumentation and Control provides a research element (§3.5.6, “Firewalls”) to address network security. While the survey identifies prominent security techniques, a thorough investigation of the subject has merit. In light of increased security awareness and the introduction of wireless communications into process control systems, recent research by NRC into the network and computing security is well justified and should proceed by addressing the full range of techniques.

In the computational platform technology focus area, real-time operating systems represent a key topic that may warrant expanded near-term research. Because operating systems provide the fundamental interface between software and hardware in most digital applications, their performance and reliability characteristics should be well understood. The NRC Research Plan for Digital Instrumentation and Control contains a research element (§3.2.6 “Operating Systems”)

that addresses the research need in this area. Therefore, the survey findings are consistent with the research plan. As an additional observation, participation by the NRC in software standards activities would prove beneficial for advocating safety considerations in real-time operating systems. Since most operating system developers focus on satisfying the wider market of less-demanding commercial and industrial applications, development of consensus approaches that emphasize safety and reliability characteristics would promote general improvements in the technology.

The NRC Research Plan for Digital Instrumentation and Control contains a research element (§3.5.2 “Predictive Maintenance/On-Line Monitoring”) that addresses surveillance, diagnostics, and prognostics. Because of the likely integration of control and diagnostics for autonomous plant operation and the expected greater reliance on surveillance and prognostic methods to facilitate predictive maintenance, the survey findings confirm the need for such research. Several developing techniques are being targeted for nuclear power applications, so it would seem reasonable to conduct research in the near-term on the capabilities that those techniques provide. In particular, methods for assessing the accuracy, stability, and reliability of diagnostic and prognostic techniques are appropriate candidates for near-term research. In addition, it is reasonable to monitor development in the technology through awareness of applications in other industries.

High-integrity software is addressed in the NRC Research Plan for Digital Instrumentation and Control (§3.3 “Software Quality Assurance”). Two key topics in that field are specifically addressed, those being software development (§3.3.1 “Investigate Objective Software Engineering Criteria”) and software assessment (§3.3.2 “Investigate Criteria for Software Testing”). The findings of the survey confirm the significance of these research topics and the need for near-term attention. Two observations for particular research subjects are that methods for development of high-integrity software using more formal software engineering methods (such as the Cleanroom approach) should be investigated and that developments in the statistics of rare events for testing and assessment of very high integrity systems should be followed.

3.2 Emerging Technologies that Suggest Potential Near-Term Research Needs

Sensor networks or fieldbus technologies are identified as candidates for near-term research in the communications media and networking technology focus area. Implementation of wireless transmitters is beginning in nonsafety applications at nuclear power plants. Networks for field devices are expected to be the norm for control and information systems in new plants. The technological evolution of the sensor market and desires to reduce cabling costs are expected to give impetus to the expanded use of sensor networks (both wired and wireless) in the nuclear power industry. As a result, it seems clear that near-term research into the safety characteristics of fieldbus technologies is warranted.

3.3 Emerging Technologies that May Warrant Long-Term Monitoring

Within the communications media and networking technology focus area, some emerging technologies are identified that have the potential for eventual migration into safety-related nuclear power applications. These are high-performance architectures and selected communications media (i.e., the network physical layer).

Architectural developments have the potential to impact the distributed computing and high-speed data processing capabilities that are likely to be prominent in the integrated, autonomous control and information systems at future nuclear power plants. These developments should be

monitored and, as capabilities mature, investigated more thoroughly in terms of performance and reliability characteristics.

NRC has experience evaluating plant communications systems based on wired and optical communications media. As projected development in each area will likely significantly increase the available bandwidth for data systems (especially if all-optical networks become possible), reliability and environmental compatibility issues will still need to be considered. Therefore, it seems reasonable to monitor the state of the technology.

In addition, trends in fundamental techniques or approaches may affect the implementation and use of networks in future nuclear power plants, so it is suggested that NRC maintain technical familiarity with the state-of-the-art in those areas. Specifically, the trend toward highly interconnected distributed computing systems for autonomous control of complex process systems suggests that the capabilities of network management solutions probably will have to be considered in the assessment of safety-related control and information systems for future nuclear plants. Also, evaluation of emerging network design approaches may become an important consideration in the review of future plants with highly interconnected, distributed computing environments for autonomous control and information systems.

Several IC technologies are identified as meriting long-term monitoring because of their significance for nuclear application or their innovation in the field. These technologies include radiation-hardened ICs, SoC circuitry, optical processors (in particular, ODSPs), and unique chip processes (i.e., vertically-stacked ICs, nanotriodes, and MEMS).

The potential impact toward facilitating smart sensors and sensor networks in containment applications in the long term suggests the value of maintaining awareness of developments for rad-hard ICs. Likewise, the potential for sensing applications using SoC circuitry that can be located in harsh environments at future reactors and then changed out (perhaps robotically) on a periodic basis provides motivation for monitoring the long-term trends in SoC development.

As noted in this report, NRC has experience evaluating optical interconnections (i.e., EO hybrids) that have been implemented in nuclear plants as part of fiber-optic communications links. Although, safety-related applications of optical processing seem unlikely in the near term, the potential increase in computational speed promised by ODSPs suggests that usage over the long term is likely. Therefore, awareness of this technology should be maintained.

The prospects of unique, versatile sensors, an environmentally (especially rad-hard) robust alternative to field effect transistors, or a dramatic improvement in circuit density represent possible long-term technological developments for ICs that should be followed. The potential for impacting safety-related nuclear power applications as a result of these developments could include previously unavailable measurements that give new insight into the plant status. Additional positive impacts of new technologies are the migration of smart sensors into the most inhospitable areas within the reactor containment, or the use of new computational power and speed to support more extensive model-based surveillance and diagnostics systems that are capable of detecting incipient failure.

Numerous control and decision techniques or approaches were surveyed. NRC has significant experience reviewing control systems based on classical control techniques. There is much less (or, in some cases, no) experience with the so-called “advanced” control techniques. However, it does not seem necessary or cost effective for each and every method to be researched to assess its performance and reliability characteristics. Instead, it seems sufficient for a general knowledge to

be maintained by following long-term developments in the investigation and application of control and decision techniques (primarily by universities and national laboratories or in other industries such as fossil power).

The most significant change that is expected in control system development for nuclear power may be the transfer of more and more of the decision-making responsibility to the I&C systems. Given the staffing and operational cycle goals of long-term deployment reactor concepts and the prospect of multi-modular plants with integrated process systems and/or control rooms, the move to highly automated control and information systems seems inevitable. Continued consideration should be given to the role of the human in nuclear plant operations (anticipating the evolution from operator to supervisor with most decisions made by the machine) and the capabilities and reliability of autonomous control systems. In particular, the industry should develop familiarity with the capabilities and configuration options of highly autonomous control systems, which will integrate control, diagnostic and decision-making functions, before the long-term deployment concepts reach fruition.

As part of the survey of computational platforms, maintaining an awareness of the emerging technology of ASICs is warranted. There have been a limited number of specialized ASIC-based applications developed specifically for the nuclear industry. In light of the potential costs for dedicating commercial software-based systems, it is possible that development of ASIC-based components for nuclear power safety applications will expand in the long term.

In the technology focus area of HSI, selected emerging technology highlights involving interaction approaches for operator support, information retrieval, control room design and assessment, biometrics and site security, and virtual reality are identified. Although HSI is not explicitly part of the NRC Research Plan for Digital Instrumentation and Control, it is observed that several interaction technologies warrant long-term monitoring and may pose research needs that may be addressed in conjunction with human factors engineering research. In particular, the expected assumption of greater decision-making responsibility by autonomous, intelligent control and information systems gives rise to a research challenge for the designers, suppliers, owners, and regulators. Participation in existing international research is reasonable and interaction with industry groups (DOE, EPRI, owners' groups) in identifying and studying the issues posed by this trend is warranted.

4. REFERENCES

- 1 J. M. Harper and J. G. Beckerley, Eds., *Nuclear Power Reactor Instrumentation Systems Handbook*, Vol. 1, TID-25952-P1, U.S. Atomic Energy Commission, 1973.
- 2 S. Seshadri et al., "Demonstration of an SiC Neutron Detector of High-Radiation Environments," *IEEE Transactions on Electron Devices*, **46**(3), March 1999, pp. 567–571.
- 3 T. D. Radcliff et al., "Constant-Temperature Calorimetry for In-core Power Measurement," *Nuclear Technology*, **132**(2), Nov. 2000, pp. 240–55.
- 4 Heintz Von Brixy and Tsunemi Kakuta, "Noise Thermometer," *JAERI Review*, 96–003, JP9607006.
- 5 J. Regan and H. Estrada, "The Elements of Uncertainty in Feedwater Flow Measurements with Three Types of Instruments," *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Washington DC, November 2000.
- 6 Herb Estrada, "General Principles of LEFM Time-of-Flight Ultrasonic Flow Measurements," <http://www.caldon.net/instruments/Library.cfm>, February 2001.
- 7 "Magnetic Flow Meter Diagnostics and Information Management Module," <http://helios.ecn.purdue.edu/~aisl/projects/magnet.html>
- 8 D. W. Miller et al., *Fiber Optic Sensors in Nuclear Power Plant Radiation Environments, Phase I*, EPRI TR-107326-V1, Palo Alto, CA, 1999.
- 9 H. Liu, D. Miller, and J. Talnagi, "The Utilization of FISO Fabry-Perot Temperature Sensors in Nuclear Power Plant Measurements," *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Washington DC, November 2000.
- 10 EPRI, *Thermographic Phosphor Strain Measurements*, EPRI TR-103867, May 1994.
- 11 T. B. Hirschfield and G. R. Haugen, *Method and Apparatus for Simultaneously Measuring Temperature and Pressure*, U.S. Patent 4,768,886, September 6, 1988.
- 12 L. E. Smith, C. Chen, and D. K. Wehe, "He, Z, Hybrid Collimation for Industrial Gamma-Ray Imaging: Combining Spatially Coded and Compton Aperture Data," *Nucl. Instrum. Methods Phys. Res. A*, **462**(3) 21, April 2001, pp.576–87.
- 13 EPRI, *Instrument Calibration Monitoring Program: Basis for the Method*, EPRI TR-123436, Palo Alto, CA, 1993.
- 14 <http://rapidio.org/home>
- 15 <http://www.infinibandta.org/home>
- 16 <http://www.intel.com/>
- 17 Anita Becker, "OC-768 and Beyond: More Integration, New Technologies Shape Future," *Integrated Communications Design*, May 2000.
- 18 J. A. Mullens, "Survey of Fieldbus Instrument Systems," ORNL/NRC/LTR-00/13, Oak Ridge National Laboratory, Oak Ridge, TN, November 2000.
- 19 Jon Severn, "Safety Fieldbus: the Time Is Right," *Industrial Networking and Open Control*, Vol. 7, Issue 1, March 2001, <http://www.industrialnetworking.co.uk/mag/v7-1/severn.html>
- 20 <http://www.as-interface.com>
- 21 ProfiBus Nutzerorganisation, e.V., "ProfiBus Profile, Fail Safe with ProfiBus (Draft)," Revision 1.0, Haid-und-Neu-Str. 7, D-76131 Karlsruhe, Germany, April 1999.

- 22 SafetyBus p Club International, e.V., “SafetyBus p – Description,” Version I, Felix-Wankel-Str. 2, D-73760 Ostfildern, November 1999.
- 23 Claudio Aun Fayad and Pedro Anisio Biondo, “Reliability with Foundation Fieldbus,” *Tech. Papers of ISA: Networking and Communications on the Plant Floor, Technology Update LIV*, ISA TECH 1999, Vol. 392, October 1999, pp. 229–245.
- 24 <http://www.as-interface.com/safety.asp>
- 25 http://www.ad.siemens.de/news/tiareport/199904/html_76/foc2_1.htm
- 26 Klaus Werner Stellwag, Speech at Press Conference, Erlangen, Germany, July 5, 2001.
- 27 http://www.mesco.de/me_profibus_p3.htm
- 28 ProfiBus Interface Center, “Connection,” August 2000, 423.461.2576 or profibus.center@sea.siemens.com (<http://www.sea.siemens.com/profibu/docs/vol61.pdf>)
- 29 <http://www.controleng.com/archives/2001/ctl0902.01/e0109p32.htm>
- 30 http://www.ad.siemens.de/news/tiareport/199904/html_76/foc2.htm
- 31 http://www.themanagementor.com/IPF/Mailers/Fieldbus_p2.htm
- 32 CXK Networks Limited, TheManageMentor, <http://www.careercommunity.co.in>, 1-8-303/48/12, Prenderghast Road Secundrabad-500003, Andhra Pradesh, India.
- 33 http://www.industrialnetworking.co.uk/mag/v7-3/f_building.html
- 34 <http://www.nwfusion.com/reviews/2001/0205rev.html>
- 35 <http://bvlive01.iss.net/issEn/delivery/prdetail.jsp?type=&oid=18990>
- 36 <http://citeseer.nj.nec.com/cache/papers/cs/13832/http://zSzzSzwww.ce.chalmers.sezSzstaffzSzsaxzSztaxonomy.pdf/axelsson00intrusion.pdf>
- 37 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci810322,00.html
- 38 <http://www.biometrics.org/>
- 39 http://www.checkpoint.com/products/security/datasheets/vpn-1_gateway_ipsec.pdf
- 40 <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>
- 41 <http://www.commoncriteria.org/>
- 42 <http://www.faqs.org/rfcs/rfc1067.html>
- 43 <http://www.opennms.org/>
- 44 http://www.3com.com/corpinfo/en_US/pressbox/press_release.jsp?INFO_ID=2006206
- 45 <http://www.lenslet.com/products/papers.html>
- 46 “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” EPRI TR-107330, Palo Alto, CA, December 1996.
- 47 J. A. Mullens, D. E. McMillan, W. B. Jatko, K. Korsah, and R. T. Wood, “Operating Systems Attributes for Nuclear Power Plant Safety Applications,” ORNL/NRC/LTR-01/11, Oak Ridge National Laboratory, Oak Ridge, TN, November 2001.
- 48 http://www.compaq.com/rfoc/_Toc466335096.
- 49 Donald Lewine, “POSIX Programmer's Guide: Writing Portable UNIX Programs,” O’Reilly & Associates, 1991, ISBN 0-937175-73-0.
- 50 www.osek-vdx.org.
- 51 J. W. Crenshaw, “Mea Culpa,” *Embedded Systems Programming*, Vol. 15, No. 3, March 2002.
- 52 www.timesys.com
- 53 www.redhat.com
- 54 A. J. Massa, “eCos Porting Guide,” *Embedded Systems Programming*. Vol. 15, No. 1, January 2002.
- 55 B. Damiano, J. E. Breeding, and R. W. Tucker, Jr., “Machine and Process System Diagnostics Using One-Step Prediction Maps,” International Conference on Maintenance and Reliability, MARCON99, Gatlinburg, Tennessee, May 1999.

- 56 T.J. Bjørlo, Ø. Berg, "Development of Plant Surveillance and Operations Systems at the
OECD Halden Reactor Project," FLINS 98, Brussels, Belgium, 1998.
- 57 B. Damiano, S. W. Kercel, R. W. Tucker, and S. A. Brown-VanHoozer, "Recognizing a
Voice from its Model," 2000 IEEE International Conference on Systems, Man and
Cybernetics, Nashville, TN, October 2000.
- 58 D. Rovero and P.F. Fantoni, "ALADDIN: A Neural Model for the Classification of Fast
Transients in Nuclear Power Plants," *Proceedings of the 3rd International FLINS
Workshop on Fuzzy Logic and Intelligent Technologies for Nuclear Science and Industry*,
Antwerp, Belgium, September 1998.
- 59 Davide Rovero, "Soft Computing Tools for Transient Classification," *Information
Sciences*, Vol. 127, Elsevier Science, Oxford, UK, August 2000.
- 60 S. W. Kercel et al., "In-Process Detection of Weld Defects using Laser-Based
Ultrasound," *Harsh Environment Sensors II*, Boston, MA, September 1999.
- 61 *Proceedings of the 1993 ANS Topical Meeting on Nuclear Plant Instrumentation, Control
and Human-Machine Interface Technologies*, Oak Ridge TN, April 1993.
- 62 *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation,
Control and Human-Machine Interface Technologies (NPIC&HMIT 96)*, Vols. 1 and 2,
Penn State University, PA, May 1996.
- 63 *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation,
Control and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, Washington
DC, November 2000.
- 64 K. J. Åström and B. Wittenmark, *Adaptive Control*, 2nd Ed., Addison-Wesley, 1989.
- 65 D. Goldberg, *Genetic Algorithms*, Addison Wesley, 1988.
- 66 Knowledge-Based Systems, 15(1-2): 103–110 Sp. Iss. Si, January 2002.
- 67 J. R. Abrial, E. Borger, and H. Langmaack, Eds., *Formal Methods for Industrial
Applications: Specifying and Programming the Steam Boiler Control*, Springer-Verlag,
1996.
- 68 L. Petre, M. Qvist, and K. Sere, "Distributed Object-Based Control Systems," *TUCS
Report*, N. 241, Turku Centre for Computer Science, February 1999.
- 69 R. A. Kisner and G. V. S. Raju, "Automating Large-Scale Power Plant Systems: A
Perspective and Philosophy," ORNL/TM-9500, Oak Ridge TN, December 1984.
- 70 P. J. Otaduy, C. R. Brittain, L. A. Rovere, and N. B. Gove, "Supervisory Control
Concepts for a Power Block with Three Reactors and a Common Turbine-Generator,"
ORNL-TM-11483, Oak Ridge TN, 1990.
- 71 P. J. Otaduy, C. R. Brittain, L. A. Rovere, and N. B. Gove, "Supervisory Control
Conceptual Design and Testing in ORNL's Advanced Controls Research Facility," *AI91:
Frontiers in Innovative Computing for the Nuclear Industry*, Vol. 1, Jackson Hole WY,
September 1991, pp. 170–179.
- 72 http://hydro.energy.kyoto-u.ac.jp/Lab/staff/shimoda/paper/EAM99_ohp.pdf , Graduate
School of Energy Science, Kyoto University.
- 73 Kenneth Tobin et al., "Content-Based Image Retrieval for Semiconductor Process
Characterization," *IEEE Quality Control by Artificial Vision*, Le Creusot, France, May
2001.
- 74 Colin Venters and Matthew Cooper, "A Review of Content-Based Image Retrieval
Systems," University of Manchester, <http://www.jtap.ac.uk/reports/htm/jtap-054.html>.
- 75 J.R. Price and T.F. Gee, "Towards Robust Face Recognition from Video," *Proceedings of
the 30th Applied Imagery and Pattern Recognition Workshop*, October 2001, pp. 94–100.

- 76 T.F. Gee, T.P. Karnowski, and K.W. Tobin, "Multiframe Combination and Blur
Deconvolution of Video Data," *Proceedings of Image and Video Communications and
Processing*, SPIE Vol. 3974, January 2000, pp. 788–795.
- 77 J.R. Price, T.F. Gee and K.W. Tobin, "Blur Estimation in Limited-control
Environments," *Proceedings of the IEEE International Conference on Acoustics, Speech,
and Signal Processing*, Vol. 3, May 2001, pp. 1669–1672.
- 78 *Proceedings of the Third IEEE International Workshop on Visual Surveillance*, July
2000.
- 79 *Proceedings of the 30th Applied Imagery and Pattern Recognition Workshop*, October
2001.
- 80 T.F. Gee and R.M. Mersereau, "Model-Based Face Tracking for Dense Motion Field
Estimation," *Proceedings of the 30th Applied Imagery and Pattern Recognition
Workshop*, October 2001, pp. 149–153.
- 81 *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and
Reliability Issues*, National Academy Press, Washington, DC, 1997
- 82 V. Basili and B. Boehm, "CeBASE: The Center for Empirically Based Software
Engineering," Twenty-Fifth Annual Software Engineering Workshop sponsored by the
NASA/Goddard Space Flight Center (GSFC) Software Engineering Laboratory (SEL)
and the IEEE Computer Society, December 4, 2000.
- 83 Stacy J. Prowell, Carmen J. Trammell, Richard C. Linger, and Jesse H. Poore,
"Cleanroom Software Engineering Technology and Process," Addison-Wesley, 1999.
- 84 http://sel.gsfc.nasa.gov/website/sew/2000/topics/Vbasili_SEW25_Slides.PDF
- 85 Jack Ganssle, "A Guide to Code Inspections," White Paper, 2001. www.ganssle.com
- 86 M.Li, and C. Smidts, *Software Engineering Measures for Predicting Software Reliability
in Safety Critical Digital Systems*, NUREG/GR-0019, 2000.
- 87 U.S. Nuclear Regulatory Commission, "Criteria for Digital Computers in Safety Systems
of Nuclear Power Plants," *Regulatory Guide 1.15*.
- 88 M.Li, and C. Smidts, "Validation of a Methodology for Assessing Software Quality,"
Letter Report, March 2002 (draft report).
- 89 M. Hecht and H. Hecht, "Use of Importance Sampling and Related Techniques to
Measure Very High Reliability Software," IEEE Aerospace 2000 Conference, Big Sky,
MT, March 2000.
- 90 J.H. Poore, personal communication, University of Tennessee, March 12, 2002.
- 91 Smith, DeLong and Johnson, "A Safety Assessment Methodology for Complex Safety-
Critical Hardware/Software Systems," International Topical Meeting on Nuclear Plant
Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT
2000), Washington, DC, November, 2000.
- 92 Real-Time for Java Expert Group, *Real-Time Specification for Java*, www.rti.org
- 93 Michael Barr, "Making Java Real," *Embedded Systems Programming*, March 2002, Vol.
15, No. 3.

Appendix A

A Nuclear Industry Perspective on I&C Technology

James R. Easter

A INTRODUCTION

This document attempts to predict where the instrumentation and control (I&C) technology that is used in commercial nuclear power plants is headed over the next ten years. The approach that is taken in making this prediction is to look at the current plant owner and vendor environments and, based upon their perceived needs and limitations, to base the prediction on the direction that the I&C *functionality* is likely to take. Then the document makes some observations as to the impact that functionality might have on the U.S. Nuclear Regulatory Commission's job in assuring the public's health and safety.

This approach has both positive and negative aspects. On the positive side, attempting to predict the revolution in I&C hardware and then to guess how that new hardware might be used in the I&C systems of nuclear power plants seems fraught with error. However, the desired improvements in capabilities/functionality that a plant operator might like to have seem much more predictable. In fact, many plant operators are now making such desires known to vendors, but it will take years for the vendors to design, install, and get regulatory approval for products which meet these desires. Similarly, the impact that a given functionality might have on a plant's licensing basis is clearer. On the negative side, there are likely to be consequences/side effects of future hardware/software technologies and designs that may well affect the safety case of their application in nuclear power plants that are currently impossible to predict. As a result, in spite of our best attempts at early warnings, there will be aspects of future I&C designs that will directly affect the safety case that cannot be predicted today.

This document develops a 'basis' for predicting the future by examining the plant owner and vendor environments to better understand what functionality the plant owners may be looking for in the next few years and to compare that against the I&C vendors' constraints in developing and providing I&C that includes the desired functionality. Once the basis is established, the author looks at the various areas of nuclear power plant operation and makes a prediction on I&C functionality improvements that would seem to be helpful, effective, and cost beneficial. Once the future functionality is described, the author makes an estimate of the issues related to the functionality that the regulatory authority might find worth reviewing in order to assure the health and safety of the public.

Throughout the remainder of this document, the discussion adopts the Electric Power Research Institute's (EPRI) Advanced Light Water Reactor (ALWR) Utility Requirements Document (URD) definition of the Man-Machine Interface System (MMIS), as it includes both the traditional plant I&C and the Human-Machine Interface as a single, integrated system.

B BASIS FOR PREDICTION

B.1 The Plant Owner / Operator's Environment

Power generation deregulation, to no one's surprise, has caused a number of fundamental changes in the way that plant owners view and, to some extent, operate nuclear power plants. Deregulation has done what it was intended to do; that is, it has forced fierce competition between the generators. This, coupled with the power shortages that have plagued various parts of the U.S. in the last couple of years, has caused power generators to drastically change their view of power generation, in general, and nuclear power generation, in particular. Power generation is no longer a 'technology' whose technological progress is

driven by engineers and technical specialists. Power generation is now a 'commodity' whose technological progress is driven by cost/benefit analysis. The implication is that the plant owners will not purchase anything that cannot be clearly shown to "add to the bottom line". Based on this view, one would not expect much to change in the near future.

On the other hand, the power shortages have pointed out to power plant owners that existing/installed generation capacity is a rather valuable commodity. This has resulted in a flurry of nuclear power plant owners rushing to the NRC to 'get on the license renewal/extension list'. In evaluating the improvements that additional years on their operating license will demand, plant owners have come to realize that serious renovation is warranted on the plant's MMIS. This is because the commercial process control instrumentation and control technology has undergone a revolution in the last decade in moving from analog to digital technology. Since the market for I&C equipment to nuclear power plants, compared to the overall process control market, is very small, the nuclear power plant owners have increasingly found it difficult and expensive to acquire replacement parts for aging analog equipment. They have also found it difficult to hire young analog equipment maintenance technicians to replace those that are retiring that have been maintaining the analog I&C equipment since 'the plant was built'. Due to market forces, the 'tech' schools are training technicians to repair digital equipment, not analog. As a result, many nuclear power plant owners, particularly those who have decided to extend their operating license, have begun to seriously consider replacing much of the I&C and control room equipment. Some have already committed to contracts with the major nuclear power plant I&C vendors, all of whom are providing digital equipment to replace the existing analog equipment.

Because of limited Operating and Maintenance budgets for any one year, along with very short outages available for equipment installation and testing, plant owners are requesting 'phased' implementations to get to an 'end vision' design. More and more, the plant owners' end-vision is becoming that found in the Advanced Light Water Reactor Plant owner Requirements Document that was put together by the Electric Power Research Institute (EPRI) during the late 1980s and early 1990s. That end-vision is a 'glass cockpit' design for the control room (i.e., operator sit-down workstations, with all process data display and process control done via computer driven Visual Display Units (VDUs)), with a fully distributed computer network architecture connecting the "front" side of the control board with the process equipment.

This is the same MMIS design that was brought to the NRC in the 1990s by the major nuclear power plant vendors and plant owners that were seeking Safety Evaluations for their 'advanced' plant designs.

As a result of these influences, the nuclear power plant owners and the owners of prospective new plants are headed toward the same concept for the design of the I&C for their plants, whether these plants currently exist or are only on the drawing board.

Because of the much increased emphasis on "the bottom line", plant owners have also begun to recognize that there is 'strength in numbers' or rather that economies-of-scale can be had in dealing with the MMIS vendors. As a result, a number of plant owner "alliances" have been formed in which several owners will contract with a vendor for similar services at all of the alliance's plants.

The emphasis on the bottom line is causing the plant owners to consider "out-sourcing" arrangements of various types. One of which is to embark on a Profit Sharing/Partnering arrangement with vendors/suppliers. These are much closer to the Japanese model of the 'vendor and customer' relationship. The current U.S. version is focused upon some form of profit sharing only. The Japanese version essentially is more like that of IBM or Xerox in the '70s in which customers did not buy the products, but rather rented them and the supplier was responsible for their operation, including all maintenance.

These forces are driving the plant owners to become much more commercially efficient with all of their power generation assets. In the next ten years, this may be the predominant force for change in the MMIS. As an example, fossil plant owners are already beginning to force decisions (and the requisite data) about the commercial side of their operation down to the Production/Shift Supervisors at the plants. These

people, who are responsible for all aspects of the plant for two-thirds of the day, are going to be responsible for making moment-to-moment decisions about plant operations / power production based upon current commercial/market conditions, e.g., the current price of a megawatt of power, the current availability of other power generation capacity on the grid, the current cost of power generation at the plant in question, etc. In the next ten years, this same effort to optimize operations can be expected to be pushed into the nuclear power plants, as well.

This typically means a desire to use the Internet to provide the data communications network. As a result, regulators can expect to see a push by plant owners to connect their Plant Information Networks (PINs) to the Internet in order to receive data about current market conditions and to transmit data about their current plant operations. Typically, these PINs, are plant-wide local-area-networks that are used for communication of plant 'enterprise' data, such as parts inventory, personnel data, local plant financial data, etc. There is a growing demand for the PINs to acquire, at least, plant process data from the MMIS, in order to up-date the enterprise applications programs with the most current data, relative to plant operations.

B.2 The Vendor Environment

Since the late 1980s, the major vendors of nuclear power plant I&C have faced a shrinking market for their products. This is in part due to some owners deciding to permanently close their plants, but is mainly due to the fact that plant owners have not been willing, until recently, to consider spending money on improving the MMIS of their existing plants. This situation, coupled with a lack of new power plant orders, has prompted an era of major consolidation of the vendors.

The major U.S. nuclear power plant MMIS vendors are now consortiums of former U.S. companies and foreign companies. The consortiums include British Nuclear Fuels Limited, Westinghouse, and Combustion Engineering – Asea Brown-Boverie (BNFL/W/CE-ABB); Framatome Advanced Nuclear Power (Framatome ANP) which is a consortium company made up of the former Babcock and Wilcox, Framatome, Kraftwerke Union, and, a recent addition, Duke Engineering and Services, Inc. (B&W/FRA/KWU/DESI); a third is Invensys, which is made up of Invensys, Triconex, and Foxboro; and, finally, Data Systems and Solutions (DS&S), which is a consortium company of SAIC (Huntsville, Ala) and Rolls Royce Electrical Systems. Only General Electric (GE) still stands alone.

Most of these vendors now are simply assemblers of I&C architectures, with the components made overseas. BNFL/W/CE-ABB and Framatome ANP get most of their digital components from manufacturers in Germany, while GE is coupled with Toshiba and Hitachi of Japan. Only Invensys still claims that their architecture of Programmable Logic Controllers (PLCs) is composed of components manufactured in the U.S.

The current level of development of the hardware technology is such that the capability of the hardware and instruction level software is far more than the MMIS designers' understand how to use most effectively. As a result, the advances in MMIS over the next ten years are expected to be in application software and in the understanding by HSI designers about how to build truly effective human-computer interfaces and decision support systems. An example is the current level of development and very low price of desktop tools for three-dimensional animation. So far, this technology's application has been to animated movies and video games. Clearly, it has application to the presentation of process data to real-time process control operators, but the applied cognitive psychologists and human-computer interaction researchers have not yet determined and set down the design principals to be used when applying the technology to the process control domain. This will undoubtedly change over the next several years.

C MMIS HARDWARE ARCHITECTURE

C.1 Current Position – Distributed Computers

Because of the international flavor of most of these MMIS vendors, most of them have a large incentive to develop a single I&C architecture that can meet the approval of regulators and be deployed in any country in the world, i.e., an architecture that will meet the needs of any plant owner and any regulatory authority in the world. Usually, this means that the protection system part, i.e., the Safety Class 1-E portion of the architecture, is custom built to meet the requisite regulatory requirements.

The Safety Class non-1-E portion, though, is currently being designed around commercial-off-the-shelf (COTS) equipment and software. Distributed computer designs can now be found in any contemporary process control plant and in fossil plant applications. Nuclear power plant MMIS vendors now have begun to offer plant owners COTS designs for non 1-E systems, often with the expectation of using the COTS technology for meeting the regulatory requirements for ‘diversity’. At least one of the nuclear power plant MMIS vendors has U.S. regulatory approval for such a design and is currently installing it at a number of operating U.S. nuclear power plants.

The overall hardware architecture that all vendors have come to is one of distributed computers (or PLCs) that are connected with data highways of various technologies and bandwidths. Often the architecture has more than one layer between the computers performing HSI functions and those that are doing the data acquisition and equipment control. This type of architecture is very conducive to expansion, since additional computing horsepower usually can be added by simply connecting to the highway. This means that the impact on the overall architecture or on the ability of existing machines to continue to carry out their functions is very small. In centralized computer systems, in the 1980s, there was always a question, for example, of the loss of response time to user requests if additional users were added to the system. This is not the case with a well-designed distributed computer network. Likewise, system reliability is better because of the ease of adding redundancy to the network.

C.2 Projected Direction Over the Next 10 Years

The basic Safety System architecture is not likely to change in the next 10 years. Vendors are still trying to recoup their development and licensing costs, and the 2/4 voting logic, with its inherent ‘installed spare’ voting channel (i.e., the voting logic is really 2/3) appears to be quite robust.

The details of ‘what is voted on’ and ‘what is done with the output’ of the voting logic may change with the advent of new plant designs, particularly if those designs are other than the traditional light water type, but the fundamental design is not likely to change.

The two big changes that are likely to develop and influence hardware architecture in the next ten years are those that are currently driving the telecommunications industry, namely, communication highway bandwidth and computer speed. Such changes will ‘make affordable’ additional capacity for use by applications programs that can aid decision making and improve plant commercial efficiency.

Finally, the capabilities of distributed hardware architectures are such that they become able to make data available to all of those who have a use for it. This, for example, might make the job of the Shift Technical Advisor (STA) somewhat easier in that he / she might be able to begin acquiring data outside of and on the way to the control room.

C.3 Anticipated Regulatory Authority Impact

For Safety Class 1-E I&C, the current architecture is proving sufficient so that fundamental issues of redundancy and diversity probably will not undergo much change. The 2/4 voting logic also is well established and proving to be robust, so there is not much need to re-think this issue. This design will be applied to both new plants and to the up-grade of existing plants. Therefore, as far as the hardware architecture of Safety Class 1-E systems is concerned, there should not be much that is new in the next ten years.

For non-Safety Class 1-E functions, the distributed computer architecture is also not expected to have much impact on or need for intensive regulatory effort. Consideration will need to be given to the use of COTS for performing these functions, and it is expected that more vendors and plant owners will want to use the same COTS technology for performing the functionality that is required by the needs for diversity in accomplishing the requisite safety functions.

D MMIS SOFTWARE ARCHITECTURE

D.1 Current Position – Distributed Computers vs. Distributed Computing

Currently, the applications (i.e., non-Safety Class 1-E) software that vendors typically incorporate on their distributed computer architectures is, to a large extent, simply ‘ported’ from the old centralized plant computer systems. Control system software is often legacy software from commercial process control applications of their COTS systems. The result is that the MMIS hardware architecture is distributed, but the software is simply brought over from some existing design, more or less intact, and is given to a processor in the architecture to perform, i.e., the hardware is distributed as a result of thoughtful design with hardware objectives in mind, but the software computing is not.

Both plant owners and vendors are gradually becoming aware of the fact that at least as much design attention should be expended in distributing the software in an advantageous fashion. Essentially, this means that current distributed computer systems often perform the same or similar calculations multiple times in multiple locations within the hardware architecture, rather than performing a calculation once and distributing the result to all of the other applications that need it. The result is that computer horsepower is being consumed to perform needless repetitive calculations, but, more importantly, such a software architecture makes for a maintenance / configuration management nightmare, particularly as the number, sophistication, and complexity of the application software expands, since corrections / modifications to algorithms, set-points, constants, etc. must be done in multiple places. Also, the same calculated variable may use two, slightly different methods of calculation in two or more places in the architecture with the potential of slightly different values for the same variable. Ensuring correctness and completeness, as part of a configuration management process, in such a situation can prove to be difficult

D.2 Projected Direction Over the Next 10 Years

As a result of these concerns, there will be pressure, both from customers and, probably, regulatory agencies to improve this situation. As a result, the next ten years is likely to see the gradual development of software architectures that utilize ‘single entry point’ data bases and software that is carefully designed and distributed within the distributed hardware architecture to take advantage of such a data base.

The result of such a design is that there is no repetitive calculation of variables and that changes to data base entries are made one time, at one location in the architecture’s data base, and all uses of it are up-

dated by the system. The impact on the time and effort required in managing and assuring consistency in the procedures, alarm logic, process variable displays, etc. is likely to be quite large.

The force that opposes such an eventuality is the expense of designing and building new software. However, a similar situation exists in the application of digital technology to commercial process control as well. So, while the movement toward distributed computing is likely to be slow, it should be continuous and will likely increase if the market for MMISs in nuclear power plants increases.

D.3 Anticipated Regulatory Authority Impact

Effort in this direction should provide real improvement in the process of executing configuration management. The drive to a single-entry-point data base, as noted above, will make the problem of executing and auditing the execution of configuration control over the MMIS more straightforward and will provide a greater level of assurance of both the necessity and sufficiency of modifications.

E MMIS NETWORK DATA COMMUNICATIONS

E.1 Current Position

The issue of what needs to be communicated is more a question of what needs to be displayed to end users than to what can be useful to other application software. In addition, data communication technology, until fairly recently, has been a ‘choke’ point in the overall throughput capability of a distributed computer system design. This limitation has also caused designers to want to limit the number of ‘types’ of end-users. Adding a workstation to a network may impose no real effect on network performance. However, if that workstation demands a different data set than the others on the network do, then that means that additional data must be added to the communications links. This can cause network performance to slump. However, recent developments of fiber optic and high speed/capacity Ethernet data communications capability has made the hardware capabilities exceed the designers understanding of how best to use it. Current vendor offerings of distributed computer networks for MMIS application in nuclear power plants include the capability to provide workstations with useful real-time process data in remote locations, such as the plant’s administration building and maintenance ‘shacks’.

E.2 Projected Direction Over the Next 10 Years

The demand for bandwidth is never ending. Today’s seemingly “unlimited” network capacity will be a design cramping limitation tomorrow. An issue that will drive the need for communications capacity upward is the relentless move toward digitizing a plant’s entire design basis along with life-cycle configuration management. This includes construction drawings, procedures for maintenance as well as operations, parts inventory records, tag-out and work order management, etc. Much of this is needed, at one time or another, in the control room and other locations, for addressing real-time operational issues/problems. Obviously, the result is that the need for data communications within a distributed computer MMIS network is going to grow.

A problem that occurs with improved throughput is often the need to change the hardware devices that perform the function. Such is likely to be the case with improved data communication bandwidth, i.e., the transmission cables are likely to need to be changed. Pulling wire in a nuclear power plant is an extremely expensive endeavor. It is currently the most costly and time-consuming part of installing a distributed computer network. As a result, the industry is continually looking at performing data communications via wireless methods. Such techniques would be particularly advantageous for data collection from sensors,

particularly for those that are located within the plant's containment and auxiliary buildings. While no MMIS vendor is currently marketing a wireless network for application to a nuclear power plant, the economic benefits over the life of the plant seem very compelling. As a result, application of wireless communications to local area networks, e.g., to the application of MMISs, seems very likely in the next ten years.

E.3 Anticipated Regulatory Authority Impact

Increasing the capacity of data communications does not seem to imply much impact on regulatory authorities. The only question is one of access. With increased amounts of plant design, construction, and operating data available through the MMIS, there will be greater pressure to provide access to it from groups and personnel that are outside the purview of the moment-to-moment control of the plant. Thus, care will need to be taken in designing the distribution of the needed data such that outside involvement in real-time plant control cannot take place.

The application of wireless network communication may be more vulnerable to invasion, both passive and active, by 'outsiders'. Therefore, the need for the application of firewalls, encryption, and other security methods will need to be thought through and appropriately applied to such designs.

F MMIS HUMAN-SYSTEM INTERFACE (HSI) ARCHITECTURE

F.1 Current Position – Digitize What Exists, in the Form that It Exists

The Human-System Interface (HSI) that is provided by most MMIS vendors today simply makes the analog HSI equipment into similar looking images on digital Visual Display Units (VDUs). For example, analog trend or strip-chart recorders in the analog HSI appear as trend graphs on VDUs, wheel-edge analog meters look like wheel-edge analog meters, etc. Similarly, analog 'auto-manual' stations used for adjusting and monitoring automatic control loops are simply duplicated in form and function on a digital screen. Few vendors seem to re-think the problem of process data display and control when moving to digital technologies. Part of the problem or dis-incentive is the 'legacy' that existing analog HSIs have, both in the end-user training and procedures and in regulatory understanding and acceptance.

Another problem that most vendors have not addressed is the integration of currently stand-alone systems, for example, the Safety Parameter Display System (NUREG-0696), the By-passed and Inoperable Status Indication System (Reg. Guide 1.47), Alarm System, Fire Protection, Radiation Monitoring, etc. This view has also avoided effective integration of the Post-Accident Monitoring System (Reg. Guide 1.97) along with the supporting Safety Class 1-E controls. There are digital PAMS systems in currently operating analog control rooms. In converting to a distributed computer network, the PAMS software is usually simply ported to the new Safety Class 1-E HSI hardware. As a result the data presentation format and navigation paradigm are usually very different from that used for normal or abnormal operations in the non 1-E HSI hardware. Safety Class 1-E process controls that might be expected to go along with the PAMS display of process data are not currently available. No vendor has a Safety Class 1-E design for process controls on the market nor one that is currently before a regulatory authority for approval. As a result, these distributed network designs expect control room operators to use VDU process data displays and VDU displayed process controls for normal and abnormal plant operations, but during design basis events they are expected to revert to a different paradigm of process data display and use traditional analog controls to execute control actions.

A similar situation exists for the presentation of operator guidance / procedures. MMIS vendors have begun to offer procedures presented on VDUs. However, the hardware for such presentation is not Safety

Class 1-E approved, so should this equipment fail during a design basis event, the operators must use a paper / hardcopy version of the procedures. Again, an HSI paradigm shift may occur during a high-stress situation.

Procedures also are an area where a new paradigm needs to be developed. Vendors, today, when computerizing procedures, leave the procedures in tact, i.e., in text form, and simply put the text on a VDU. Sometimes the design is nothing more than a 'page turner'. At best, the computerization will also present the relevant process data and make decisions about whether or not the current data meets the procedure step's demands / expectations, but the procedure is still the same text that was originally presented on paper. Computers and digital graphics technology offer much better means for presenting guidance to the operators. However, the principles for appropriately developing a new paradigm for guidance presentation are not currently available. Some additional research is necessary.

Alarm Systems are another area where the computer technology has not been utilized effectively. Currently, MMIS vendors are simply taking the labels from annunciator tiles, porting the logic and these labels / messages into a computerized VDU display of chronological lists of messages that can be parsed, upon user demand, into various sub-lists. There is no commercially available system to use computer technology to improve the human operator's ability to understand the context surrounding a message or to improve the content of the message.

Alarm systems, in analog control rooms, perform the function of focusing the control room's staff on a 'problem at hand'. MMIS vendors are beginning to explore the use of large screen VDUs to perform this task in computerized control rooms. That exploration is only beginning. It is not clear, for example, what an effective 'alarm system' design is when such a medium is used as the primary means of presentation.

F.2 Projected Direction Over the Next 10 Years

One can expect that vendors will make more use of the emerging discipline of Cognitive Systems Engineering to take better advantage of the capabilities of computer technology to improve the effectiveness of the HSI. The realization that everything is now "a display" is only now beginning to dawn on vendors and plant owners. The result of this realization should be a better integration of process data, making the end-users need for searching or finding data easier and presenting more effective contexts for better comprehension. For example, the need in analog control rooms to make the 'alarm system' a separate, stand-alone system was because of the nature of the technology available to execute logic. Modern computers can do a far better job of executing logic, which permits much more robust logical expressions. A great improvement in the effectiveness of alarm indications can be made by being very careful to write a logical expression that defines, exactly, the operational region of abnormality. This will greatly reduce the 'cry wolf' syndrome that most analog alarm systems currently have.

In addition, there is no need in a computerized environment to make alarms or abnormality indications a separate and distinct video display set. Such data should be more thoroughly integrated into the process data presentation. Yes, there probably needs to be separate computational equipment that is dedicated to executing abnormality indication logic, but the results of such calculations should be made available, through the network for any application software to make use of it. The next ten years will undoubtedly see significant progress in more fully and effectively incorporating abnormality indication into process graphical displays.

Because of the tremendous computational capability offered by digital systems, there will be significant progress also made in providing more abstract representations of the process state, thus relieving the human operators from having to bear the mental workload of doing so. For example, computerized MMISs can represent the process state in terms of mass and energy balances, can check an entire valve alignment, and can relate these two representations. As a result, operators will be able to directly apply the theoretical understanding of the process that they learn in their training. The MMIS will support such. The

result will be that operators will be able to find and understand problems faster, and take appropriate corrective action sooner. This will mean that process deviations will be shorter and will have milder consequences.

Along this same line, vendors and plant owners will extend the *functional* view of the plant processes that is currently represented by the Critical Safety Function view from NUREG-0696. Extending this view into normal, abnormal, and severe accident management modes of operations and implementing it in the MMIS (including the organization and content of the corresponding procedures) will make the transitions across operating modes, within the MMIS, much more seamless and ‘bumpless’. This will permit the development of operator habits in finding and interpreting process data and exercising process control that are effective across all modes of plant operation. This will surely make for a more reliable operator, since there is a reduction in possible sources of human error.

By abstracting and aggregating process data, the MMIS can reduce the number of pieces of data the human operators need to concern themselves with when performing their operational duties. This is an effective way to reduce the data overload that plagues the analog control rooms of today.

Rather than make existing decision support systems such as SPDS, BISI, Fire Protection, Radiation Monitoring stand-alone, separate systems, in a computerized MMIS, designers should begin to think about the *functionality* that is required and incorporate it in the design of displays. This should provide the data from these systems with more contexts and make the meaning of the data more accessible and useful to operators. They will not need to hop around from one system or display set to another, trying to remember what it is they are looking for or what it was that they found.

Procedures will be recognized for what they are, a method for providing operators with operational guidance. This will encourage the development of new methods for doing such, utilizing the capabilities of computer technology. A simple example is the issue of ‘valve line-ups’. Currently, the directions for aligning the valves correctly so as to get flow from one desired point to another is a series of textual lines that include the valve tag number and its desired state. By using computer graphics, one can simply show the requisite valves and identify on the graphic those valves that need to change state in order to provide the desired flow path. A picture is, indeed, worth a thousand words!

The next ten years is likely to see more of the operation of local panels brought into the control room. So, as the data overload is addressed on one front by improving the presentation and context for data, on another there will be more of it with which to deal. This will be driven by a desire of plant owners to reduce plant staffs by eliminating some or all of the auxiliary operators.

There will be demand by end-users to “own” their interfaces. This means being able to make changes, off-line, to improve the tools with which they do their jobs. As a result, vendors will need to provide computerized support tools that do not need software engineers or programmers to make them work. The HSIs for these tools will need to be simple to use and will need to be in the language of the end-user, not a programming language.

F.3 Impact on Human Communications

In analog control rooms of today, verbal communications between control room members is most often about data, “What is the temperature?”, “What is the control setting?”, “What is the valve position?”, etc. that is driven by the text based procedures. With MMIS’s that gather and present such data as a part of well designed displays, such questions and related discussion are no longer necessary. Control room verbal communications can move to a ‘higher plane’, i.e., can begin to really discuss the nature of the plant’s problem, its implications in terms of time and effects, and possible solutions, rather than on the search for data. This should improve control room performance.

F.4 Anticipated Regulatory Authority Impact

Fundamentally, such improvements in the MMIS may well mean that the review checklist found in NUREG-0700, Rev. 1 is inadequate and needs to be up-dated. Most of all, it is not clear that the underlying principles for designing and evaluating display sets to ensure that they will, in fact, provide the kinds of improvements that have been discussed are currently available. Additional research is likely to be necessary. Without principled guidance, vendor designers and plant owners may not achieve the desired improvement.

G MMIS FOR MAINTENANCE – OF THE PLANT AND OF THE MMIS

G.1 Current Position – Digital REALLY is Different From Analog

Currently, plant maintenance, mechanical, electrical, and I&C, is of the ‘periodic’ or ‘preventive’ variety. Tests are performed periodically and maintenance is done accordingly in order to prevent failures from happening during operation. The periods for testing and maintenance are typically scheduled so as to fully anticipate the equipment’s mean-time-to-failure. However, there are criticisms that this causes equipment to wear out just due to the testing and that equipment is repaired / re-built when, in fact, it could have run a significant amount of time further without failing. As a result, plant owners are looking for a less intrusive and more exact way of anticipating when to do maintenance.

Many plant owners seem to feel rather uncomfortable with digital systems. While most plant owners have some digital systems, they usually are of the mainframe variety and are seldom considered to be essential to plant operations. There are some exceptions. There are some plants that do have digital systems that are performing the Post-Accident Monitoring System functions. Owners, in some sense, are being driven toward digital systems for their MMIS functions due to problems with the obsolescence and expense of analog equipment, and difficulty in replacing retiring analog maintenance personnel. As a result, plant owners are acknowledging that ‘digital is the way to go’, but feel that they are not completely prepared to ‘jump in with both feet’. This is particularly true for the HSI portion of digital MMISs. The maintenance aspects of digital HSIs, i.e., human factors and verification and validation issues related to HSIs, is unknown territory for most plant owners.

In today’s plants, operations staff have a difficult time keeping track of the impact of maintenance on operating systems. For the most part, communications is done via paper work in the form of the ‘tag-out and work order process’. This has, on occasion, caused operators to be ‘surprised’ by such things as where maintenance personnel are in the plant, what equipment is currently being tested, exactly when maintenance is to be done, etc. One of the biggest problems is the analysis of ‘limiting conditions for operations’ during plant outages. This is caused by the unusual configurations of mechanical and electrical equipment that can occur during an outage due to the demands of maintenance. Currently, plant owners do not feel that any MMIS vendor has a truly useful / effective computerized tag-out and work order tracking system available.

Currently, end-users of HSIs have little involvement with the up-keep / improvement of the tools that they use to do their jobs. For example, operators had very little to do with the design of the analog control boards which they operate and getting operator initiated changes made in sheet metal with analog devices is very difficult. As a result, most operators do not feel much ownership of the boards, i.e., the tools of their trade, or have much sense that they can get real improvements made to them. One of the proven tenets of applied cognitive psychology is that ‘ownership improves performance’.

G.2 Projected Direction Over the Next 10 Years

Equipment maintenance is headed toward 'predictive' maintenance. This type of maintenance uses 'failure signatures' as a basis for determining when a piece of equipment will fail. These signatures are provided by equipment manufacturers based upon test-to-failure of their equipment while being well instrumented. The 'signature' is the behavior of the sensor data just before failure. Plant owners can then install the same sensors and use pattern matching on the time history of the sensor data to establish an early, but not too early, warning of when equipment is about to fail. This is the sophisticated, modern day equivalent of 'the squeaky wheel gets the attention'.

Such maintenance practices will impact the MMIS by increasing the number of sensors that must be accommodated and by providing the computational capability to track the data and look for signatures. The result is certainly in the purview of maintenance personnel, so is likely to be displayed in their offices and maintenance facilities. Some of it is also likely to be displayed in the control room, so as to provide operators with early indication of impending equipment failure, and, at the very least, to aid them in performing investigations to determine the limiting conditions for operation that are available if maintenance is to be performed. Such cross-fertilization of data will aid in bridging the gap between maintenance and operations.

The tag-out and work order process is ripe for effective computerization. Most maintenance requests are initiated in the control room. As discussed above, the control room is also most impacted by the maintenance that they have requested. As a result, there is a great desire in the control room for on-line tracking capability of the requested maintenance. This will surely come in the next 10 years. Along with this will come aids in determining the acceptable LCO configurations.

Digital technology offers unprecedented capability to make maintenance of MMISs more reliable and efficient. This is because the MMISs can perform large quantities of self-checks and can offer self-diagnoses that are presented in well-designed HSIs. This includes presenting the results in 'plain English' rather than in 'computer-ese', such as hexi-decimal or memory maps, etc.

Software maintenance, particularly that which builds and modifies the HSI, requires building effective maintenance tools. The 'knowledge base / inference engine' paradigm for separating domain specific data from the software that works on it that was developed during the Artificial Intelligence era of computer science in the 1980s will manifest itself in deterministic software for use in the HSI portion of digital MMISs. This means that the 'personality' of the HSI will be contained in the 'plant specific' data file that is built and modified off-line and then loaded into the run-time MMIS system. If the tools are properly designed, this will mean that end-users can become 'owners' of their interfaces and can continually work toward making them the tools that they need to improve their effectiveness at doing their jobs. This means that the tools themselves must have interfaces that are designed with these end-users in mind, i.e., they must not need to be software engineers to use them.

G.3 Anticipated Regulatory Authority Impact

In general, the gap between operations and maintenance will close in the next ten years with the application of digital technology for maintenance use. Clearly, this adds data to the MMIS whose use in displays must be well designed. Again, as with the inclusion of enterprise data, discussed earlier, more data will tend to exacerbate the 'data overload' problem. As a result, regulators are likely to need better means for determining that the added data has been displayed effectively, that it is reasonable to expect end-users to quickly and efficiently turn the display of the data into useful information.

H.1 Current Position

Currently, nuclear power plant operators' feel that they are flying blind on the secondary side. Things happen 'over there' and the small closed loop control systems (i.e., thermostats, manostats, etc.) are executing control actions before the operators are aware of any problem. The result is that operators tend to "catch" secondary-side initiated transients only after the transient has propagated to the primary side. Therefore, the transient has had a chance to grow before operators can exercise control over it. There is a growing awareness among plant owners that improvements in the instrumentation on the secondary side may well be worth the money. By improvement, owners do not necessarily mean 'additional' sensors, but rather getting both an analog and a digital signal out of a bi-stable, such as a thermostat or manostat.

The current limitation in putting in more sensors for maintenance is the number of remaining containment penetrations and the amount of transmission / communications highway (i.e., wire) that would need to be installed.

H.2 Projected Direction Over the Next 10 Years

Over the next ten years, nuclear power plant owners are likely to begin to retro-fit the secondary-side with dual output bi-stables. These instruments continue to provide a bi-stable output that meets the needs for the existing local control loops and provides a second output that is the analog input to the bi-stable. This analog output will provide input to alarm algorithms and trend graphics that will aid operators in seeing secondary-side transients as they happen and should enable them to address them on the secondary-side and be better prepared to address their consequences when those consequences propagate to the primary side (in the case of PWRs) or back to the reactor systems (in the case of BWRs).

Any new plants that are ordered or constructed in the next ten years are likely to see these instruments installed as part of the original OEM equipment.

As noted in the previous section, the drive to predictive maintenance is going to be the major drive for additional sensors throughout the plant in the next ten years.

Additional instrumentation needs transmission. As noted earlier, transmission is very difficult and costly. In the next ten years, the industry will be looking at wireless means for installing that transmission capability.

H.3 Anticipated Regulatory Authority

As with the forces that have been discussed in previous sections relative to the drive to make more data available, the need for more sensors, i.e., more data, will tend to magnify the existing situation of end-user 'data overload' unless the display of that data is well engineered. The additional data, if not properly presented, will make using the existing data less efficient and effective, as well as being of minimal effectiveness itself. As a result, the implementation of an effective HSI engineering program to design the effective presentation of data will be even more important than it is today.