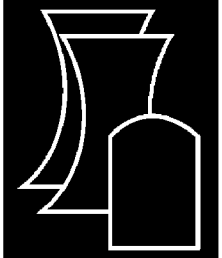
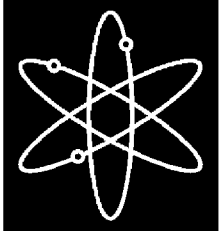
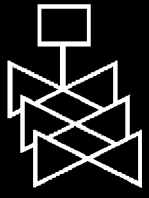
NUREG/CR-6842
ORNL/TM-2004/74







Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants

Oak Ridge National Laboratory

Preferred Licensing Services

Longenecker & Associates

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

NUREG/CR-6842
ORNL/TM-2004/74

Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants

Manuscript Completed:March 2004
Date Published: April 2004

Prepared by
R. T. Wood, S.A. Arndt (NRC)
J.R. Easter (Preferred Licensing Services)
K. Korsah, J.S. Neal, E.L. Quinn (Longenecker & Associates)
G.W. Remley (Consultant)

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

Preferred Licensing Services
P.O. Box 14431
Pittsburgh, Pa 15239-0431

Longenecker & Associates
P.O. Box 3094
Del Mar, CA 92014-6904

G.W. Remley
205 Harrow Drive
Pittsburgh, PA 15238-2530

S.A. Arndt, 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 Y6478

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

ABSTRACT

This report presents the findings from a study of experience with digital instrumentation and controls (I&C) technology in evolutionary nuclear power plants. In particular, this study evaluated regulatory approaches employed by the international nuclear power community for licensing advanced I&C systems and identified lessons learned. The report (1) gives an overview of the modern I&C technologies employed at numerous evolutionary nuclear power plants, (2) identifies performance experience derived from those applications, (3) discusses regulatory processes employed and issues that have arisen, (4) captures lessons learned from performance and regulatory experience, (5) suggests anticipated issues that may arise from international near-term deployment of reactor concepts, and (6) offers conclusions and recommendations for potential activities to support advanced reactor licensing in the United States.

CONTENTS

Tables

EXECUTIVE SUMMARY

This report presents the findings from a study of experience with digital instrumentation and controls (I&C) technology in evolutionary nuclear power plants. In particular, this study evaluated regulatory approaches employed by the international nuclear power community for licensing advanced I&C systems and identified lessons learned. The report (1) gives an overview of the modern I&C technologies employed at numerous evolutionary nuclear power plants, (2) identifies performance experience derived from those applications, (3) discusses regulatory processes employed and issues that have arisen, (4) captures lessons learned from performance and regulatory experience, (5) suggests anticipated issues that may arise from international near-term deployment of reactor concepts, and (6) offers conclusions and recommendations for potential activities to support advanced reactor licensing in the United States.

Experience with advanced I&C technologies at evolutionary nuclear power plants has shown that safety-related systems incorporating this technology can be developed and licensed for commercial nuclear power plants. However, licensing issues have arisen and some design and performance issues have been experienced. Many of these issues can be attributed to uncertainties regarding the safety significance of unique physical, functional, and performance characteristics introduced by this new technology. Existing requirements and regulatory guidance focus on current generation plants and have a tendency to be prescriptive with assumptions about particular design approaches.

To prepare for review of future reactors, the U.S. Nuclear Regulatory Commission (NRC) initiated this study to evaluate current practices and capture lessons learned. This study is intended to contribute to a determination of what assumptions or technical bases may need to be changed to prepare for licensing future reactors.

Although several new or unique I&C systems and methods will be used in advanced reactors, many of these will not be of regulatory concern. Additionally, the current review methods may be adequate for the review of many of these new technologies. However, as pointed out in the National Research Council study[1], the NRC regulations and review methods may unnecessarily limit new design features, or prove difficult to implement for new technologies or plant applications.

The primary recommendation of this report is that the NRC should review current regulations. The NRC should review the appropriate regulatory guidance found in the NRC Standard Review Plan (NUREG-0800), regulatory guides (RGs), and branch technical positions (BTPs). As appropriate the NRC should determine the need to revise its regulatory guidance (or determine whether rulemaking may be needed). Areas for review include the following:

- main control room design reviews
- human system interfaces
- displays and soft controls (RG 1.47)
- post-accident instrumentation (RG 1.97)
- alarms

---

[1] National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plant, Safety, and Reliability Issues." National Academy Press, Washington, DC, 1997.

- system isolation and cyber security
- system architecture
- network communications
- software common-cause failures
- redundancy, diversity, and defense in depth
- sensors
- information and data management
- software tools, including change control and security
- system reliability
- commercial off-the-shelf (COTS) systems

These and other issues are of concern in the design, construction, and licensing of the evolutionary plants and may be issues for the NRC in the licensing of the next generation of U.S. nuclear power plants.

FOREWORD

By

The United States Nuclear Regulatory Commission

The next generation reactors will be the first opportunity for vendors to build new reactor control rooms in this country. The advances made in the development of many current generation operating reactors in other parts of the world will be used in the design and construction of new plants. These new plants are expected to have fully integrated digital control rooms, at least as modern as the N4 reactors in France or the advanced boiling-water reactors in Japan. In addition, the desire for much smaller number of control room staffs will push the designs of the plants in the direction of a much higher degree of automation (e.g., the changes in the fossil-fired power plants). The future use of multiple modular plants may also require more complex controls.

The national and international research community has been involved with research and development of advanced controls and monitoring systems for nuclear power plants for many years. The international community, particularly in Europe, Japan, and Korea, have developed integrated advanced control rooms. They have also performed more research in automation of plant operations, and advanced plant monitoring and diagnosis than in the US. Therefore, there will be significant opportunities to learn from the international experience in this area.

As part of its planning for the possible review of advanced reactors, the U.S. Nuclear Regulatory Commission (NRC) determined that a study of these lessons should be the first part of a multi-year program to develop the regulatory infrastructure (review methods and tools) to support the review of advanced instrumentation and control (I&C) systems in future reactors. The Office of Nuclear Regulatory Research (RES) sponsored this study to develop insights based on the experience that other countries have had in reviewing and licensing of evolutionary reactors. The NRC intends this study to contribute to a determination of what assumptions or technical bases may need to be changed to prepare for licensing future reactors. Additionally, it will be used to further develop the regulatory infrastructure plan and reassess the planned research program for advanced reactor I&C.

The recommendations presented in this report will be used as an input to the development of the new plan for digital I&C research and as one input for the determination as to what parts of Chapter 7, "Instrumentation and Control" of the standard review plan should be revised or revisited to support advanced reactor reviews. This report is intended to support the review of current research plans and potential revisions to regulatory guidance. However, the reader is cautioned that the recommendations are only one input to possible revisions to future research or regulatory guidance, and should not be assumed to predict future regulatory activities.

ABBREVIATIONS

ABB	Asea Brown-Boveri Corporation
ABWR	advanced boiling-water reactor
ACR	Advanced CANDU Reactor
AC160	Advant Controller 160
AC450	Advant Controller 450
AECL	Atomic Energy of Canada, Ltd.
Al	aluminum
ALARP	as low as reasonably practicable
ALWR	advanced light-water reactor
ANIS	ANlage (i.e., plant) information system
ANRE	Agency of Natural Resources and Energy
AOCS	Advant Open Control System
APWR	advanced pressurized-water reactor
AS	automation system
ASIC	application-specific integrated circuit
ATWS	anticipated transient without scram
BE	British Energy (formerly the Central Electricity Generating Board, CEGB)
BNI	basic nuclear installation
BOP	balance of plant
BTP	branch technical position
BWR	boiling-water reactor
CANDU	Canada Deuterium Uranium (nuclear power plant design)
CEGB	Central Electricity Generating Board (CEGB), now British Energy (BE)
CFR	*Code of Federal Regulations*
CNSC	Canadian Nuclear Safety Commission
COMPSYS	computer-based systems important to safety (database)
COTS	commercial off-the-shelf
CRIEPI	Central Research Institute for the Electric Power Industry
DAS	diverse actuation system
DCC	digital control computer
DGSNR	Nuclear Safety and Radioprotection (Direction Générale de la Sûreté Nucléaire et de la Radioprotection)
DILS	digital interposing logic system
DPCS	digital plant control system
DPPS	digital plant protection system
DPS	diverse protection system
DTM	digital trip module
EdF	Electricité de France
EPIX	Equipment Performance and Information Exchange (database)
EPRI	Electric Power Research Institute
ESFAS	engineered safety features actuation system
FDDI	fiber distributed data interface
GT-MHR	gas turbine modular helium reactor
HICS	high-integrity control system
HMI	human-machine interface
HSE	health and safety executive

HSI	human-system interface
HSK	Swiss Federal Nuclear Safety Inspectorate (Haupabteilung fur die Sicherheit der Kernanlagen)
I&C	instrumentation and controls
IAEA	International Atomic Energy Agency
IC	integrated circuit
ICS	integrated control system
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
INTD	international near-term deployment
I/O	input/output
IPS	integrated protection system
IPSN	Institute for Nuclear Protection and Safety (Institut de Protection et de Sûreté Nucléaire)
IRIS	International Reactor Innovative and Secure
IRSN	Institute of Radiological Protection and Nuclear Safety (Institut de Radioprotection et de Sûreté Nucléaire)
ISCO	Integrated System for Centralized Operation
KINS	Korea Institute of Nuclear Safety
KNGR	Korean next-generation reactor
MCR	main control room
MELCO	Mitsubishi Electric Corporation
METI	Ministry of Economy, Trade, and Industry
MEXT	Ministry of Education, Culture, Sports, Science, and Technology
MHI	Mitsubishi Heavy Industries, Ltd
MOST	Ministry of Science and Technology
NEA	Nuclear Energy Agency
NIC	Nuclear Information Center
NII	Nuclear Installations Inspectorate
NISA	Nuclear and Industrial Safety Agency
NOK	Nordostschweizerische Kraftwerke (AG of Baden, Switzerland)
NPL	nonprogrammable logic
NRC	U.S. Nuclear Regulatory Commission
NSC	Nuclear Safety Commission
NSD	Nuclear Safety Directorate
NSSS	nuclear steam supply system
NUPEC	Nuclear Power Engineering Test Center
OCS	operational control system
OECD	Organization for Economic Cooperation and Development
OLU	output logic unit
OPG	Ontario Power Generation, Inc.
OPG/AECL	standard for engineering of safety-critical software
OPRI	Office de Protection Contre les Rayonnements Ionisants
P&ID	piping and instrumentation diagram
PBMR	Pebble-Bed Modular Reactor
PCDIS	plant control data and instrumentation system
PLC	programmable logic controller
PPIS	plant protection and instrumentation system
PPS	primary protection system

PROM	programmable read-only memory
PRPS	primary reactor protection system
PWR	pressurized-water reactor
RAC	Reliability Analysis Center
RAM	*random access memory*
RCC	EdF and Framatome design and construction rules
RFS	basic safety rules
RMU	remote multiplexing unit
RPS	reactor protection system
SAP	safety assessment principle
SDS1	Shut Down System #1
SDS2	Shut Down System #2
SKI	Swedish Nuclear Power Inspectorate (Statens Kärnkraftinspektion)
SPIN	numerical integrated protection system
SPS	secondary protection system
SSLC	safety system logic and control
SÚJB	State Office for Nuclear Safety (Státni Úřad pro Jadernou Bezpečnost)
TLU	trip logic unit
V&V	*verification and validation*
VDU	visual display unit
VLSI	very large-scale integrated circuits
VVER	water-cooled water-moderated power reactor
W	Westinghouse
WDPF	Westinghouse Distributed Processing Family
WELCO	Westinghouse Electric Company
YGN	Yonggwang Nuclear Power Station

1. INTRODUCTION

This report presents the findings from a study of experience with digital instrumentation and controls (I&C) technology in evolutionary nuclear power plants. In particular, this study evaluated regulatory approaches employed by the international nuclear power community for licensing advanced I&C systems and identified lessons learned. The report (1) gives an overview of the modern I&C technologies employed at numerous evolutionary nuclear power plants, (2) identifies performance experience derived from those applications, (3) discusses regulatory processes employed and issues that have arisen, (4) captures lessons learned from performance and regulatory experience, (5) suggests anticipated issues that may arise from international near-term deployment of reactor concepts, and (6) offers conclusions and recommendations for potential activities to support advanced reactor licensing in the United States.

1.1 Objective of the Study into Experience with Digital I&C Technologies at Evolutionary Reactors

Existing requirements and regulatory guidance focused on current generation plants. They generally are prescriptive with assumptions about particular design approaches. To prepare for the review of future reactors, the U.S. Nuclear Regulatory Commission (NRC) initiated this study to review current practices and to capture lessons learned. This study is intended to contribute to a determination of what assumptions or technical bases may, or perhaps should, change to prepare for licensing future reactors. For example, are technologies available that would permit the NRC to relax the requirement to separate control and safety systems, and what is the potential impact of reduced plant staffing on safety-related operational and/or maintenance issues?

To provide the desired technical foundation, this investigation reviewed design, licensing, and operating experience with I&C systems in evolutionary plants (e.g., Chooz B, Kashiwasaki-Kariwa Units 6 and 7, Darlington, and Sizewell B). The primary focus of this study was driven by the following questions:

- How did international regulators license these reactors?
- What regulations, requirements, and guidance were used?
- How is the international approach for licensing digital I&C different from that used by the NRC?
- What has been the operational experience at the plants and what changes to current NRC guidance may be required?
- Given what we know now about I&C technology, what will be the big issues for the next generation of U.S. nuclear power plants?

1.2 Research Approach for the Study

This study was broken down into three concurrent tasks. Task 1 identified the relevant advanced I&C technologies in evolutionary reactors and projected the potential application of those technologies in future U.S. reactors. Task 2 captured lessons learned from the operational and regulatory experience with advanced I&C technology. Finally, Task 3 determined the regulatory approaches employed in addressing advanced I&C technology and their relation to current U.S. regulatory processes.

The information obtained was limited by availability and access. Thus, the amount of quantitative data that could be obtained was sparse. In addition, the level of detail for the findings focused mainly on high-level concerns. Specifically, those concerns included the I&C experience at the evolutionary plants; the types of problems in the design, implementation and licensing of those systems; and how the international experience relates to applications of this technology in U.S. reactors. In trying to understand the lessons learned, the study considered problems that have occurred, as well as potential issues that may emerge (e.g., technical issues, interface issues, codes and standards issues).

A technology list was established to guide the study of advanced I&C applications and experience in evolutionary reactors. The topics are as follows:

- commercial dedication
- configuration management
- diversity and defense-in-depth
- impact of support systems or tools on safety
- information management
- sensors (new parameters, networks)
- software
- standards
- system architecture
- system classification (what safety significance was assigned)
- system reliability
- testing philosophy (design for test, onboard testing)

The conclusions and recommendations reflect two considerations: First, does this pose an open issue because it has not been looked at before? Second, is this technology/method likely to be used in the next generation of U.S. reactors?

1.3 Structure of the Report

Section 2 presents the technical background and an overview of the advanced I&C technologies at evolutionary nuclear power plants. This section is organized according to technology topics derived from the list of technology focus areas (above) that were used to guide the study. The coalescing of the technology list into general technology groupings for Section 2 resulted from the determination of a limited set of technical areas for which there were significant findings. Rather than providing exhaustive dissertations for the I&C systems of each item on the technology list of each reactor studied, this study's approach was to document only significant findings, based on innovative application or substantive differences with U.S.

experience. Therefore, not every I&C system is described for each evolutionary plant, but each plant and its significant I&C applications are presented under the relevant technology topics for which it provides some notable insight. The authors believe that this organization emphasizes the relevant information so that it can be more directly related to the conclusions and recommendations derived from this study. Section 8 provides references for readers who want more comprehensive descriptions of the full I&C systems.

Section 3 identifies experience associated with the advanced I&C applications described in Section 2. In particular, this section focuses on unique characteristics of the advanced technology or technical methods that contributed to the success or failure of particular applications. In addition, this section presents the performance experience for advanced I&C at evolutionary nuclear power plants for the few cases where noteworthy information was available.

Section 4 establishes the regulatory context in which these advanced I&C technologies were licensed and the regulatory approaches employed in the review and licensing of those technologies. First, this section gives a high-level overview of the regulatory process for countries where advanced I&C systems have been licensed at evolutionary plants. The intent is not to give a tutorial on the full regulatory structure for every country, but rather to highlight the unique aspects of specific regulatory approaches. Next, this section identifies specific issues that have arisen in licensing processes and discusses the particular approaches developed to address those issues.

Section 5 documents lessons learned from performance and regulatory experience with advanced I&C technologies. In particular, this section discusses the evolution of design and regulatory approaches and summarizes the current findings from an international assessment of the U.S. regulatory framework for digital I&C.

Section 6 documents potential issues that may arise from international near-term deployment of reactor concepts based on unique advanced I&C systems characteristics and conditions that they present.

Finally, Section 7 offers conclusions drawn from an assessment of the current NRC regulatory processes applicable to the licensing of advance I&C systems. It also provides recommendations concerning the U.S. regulatory approach for evaluating safety-related advanced I&C that could be enhanced to support the licensing of next-generation nuclear power plants.

2. TECHNOLOGY SUMMARIES

2.1 Technology Introduction

This section gives technical background regarding the application of advanced I&C technology in evolutionary nuclear power plants. This overview describes digital I&C architectures, components, and design features employed in existing plants as either upgrades or new full-system implementations. This section also contains information regarding I&C designs for advanced gas-cooled and light-water reactors. The structure of this section highlights significant aspects of these advanced I&C technology applications. First, the plants surveyed in this study are identified. Then, the technology overviews of the advanced I&C applications are presented. These technology summaries highlight the high-level I&C advances made in reactors of interest.

The reactors reviewed fall into several categories. The pressurized water reactor (PWR) I&C technologies reviewed in this report are the British Sizewell B plant [Westinghouse (W)], the Swiss Beznau plant (W), the French N4 Series (Framatome), and the Temelin water-cooled water-moderated power reactor (VVER) in the Czech Republic. The boiling-water reactor (BWR) I&C technologies reviewed are the Orskashamn I plant in Sweden, Kashiwazaki-Kariwa advanced boiling-water reactor (ABWR) plant in Japan, and the Lungmen ABWR under construction in Taiwan. The Canada Deuterium Uranium (CANDU) nuclear power plants reviewed include the early Point Lepreau and Gentilly plants in Canada, Wolsong in Korea, and Embalse in Argentina, as well as the more recent upgrades at the Darlington plant in Canada and the recent deployments for the Quinshan plant being constructed in China. In addition, the I&C design advances proposed in several advanced reactor designs were also studied. These included the Westinghouse AP 600/1000, the Advanced Pressurized Water Reactor and the high-temperature gas reactor designs, the Gas Turbine Modular Helium Reactor (GT-MHR) and the Pebble Bed Modular Reactor (PBMR).

2.2 I&C Designs in Evolutionary Nuclear Power Plants

2.2.1 Sizewell B

Sizewell B is Britain's first pressurized-water reactor power station. The power station is located on the Suffolk coast of England. Sizewell B began commercial operation in May 1995, and represented a significant change in commercial nuclear power station technology for the United Kingdom (UK). Previous UK nuclear power stations were based on gas-cooled reactors.

The overall I&C architecture of Sizewell B is thought of in three groups. The first group consists of the online control systems, which regulate plant operation under normal circumstances, using closed-loop control functions to control, for instance, the reactor power. The second group consists of the controls and instruments in the main control room (and auxiliary panels). These allow the operating staff to supervise and control the operation of the plant. The third group comprises the reactor protection system.

Most of the elements of first two control and instrumentation groups are usually referred to together using the term "Integrated System for Centralized Operation" (ISCO) to reflect the

functional integration of the design. This is manifested in the ISCO object-oriented functional specification. The ISCO is implemented by three microprocessor-based systems. The first system is the High-Integrity Control System (HICS), which is based on Westinghouse Integrated Protection System (IPS) and Integrated Control System (ICS) technologies. The second system is the Distributed Computer System, which is based on Westinghouse Distributed Processing Family (WDPF) technology, a commercially distributed digital control and supervisory system product line. The third system is the Plant Control System, which is based on the combined technologies of the WDPF and the turbine control system fabricated by General Electric of England. In order to meet regulatory separation requirements, the distributed microcomputer elements of the ISCO system communicate using six data networks.

The reactor protection system functions are performed by two separate and independent systems, known as the Primary Protection System (PPS) and the Secondary Protection System (SPS). The PPS is based on the Westinghouse IPS, and the SPS is based on the British Energy/GEC "Laddic" technology. The Laddic performs logic by connecting dynamic (pulse-based) elements that perform various logic functions. Sizewell B has two sets of four-way redundant protection sensors, two sets of four-way redundant protection electronics, and four trains of safety features equipment. Each of the four-way redundant collections is referred to as a separation group.

As to classifications established by the Institute of Electrical and Electronics Engineers (IEEE), all parts of the reactor protection system and portions of the second group would be classified as 1E. Specifically, the 1E portions of the second group are the manual component controls of the safety features devices and the post-accident monitoring part of the displays of safety parameters. Load shedding and emergency load sequencing is also a separate 1E system. At Sizewell B, this system is classified as an electrical system. Except for the SPS, plant protection, control, and information presentation are implemented using distributed microprocessor-based systems.

2.2.2 Beznau NOK ANIS

The Swiss Beznau Nuclear Power Plants, KernKraftwerke Beznau I and II, are owned and operated by the Nordostschweizerische Kraftwerke (NOK) AG of Baden, Switzerland. The plants are 350-MWe PWRs built by Westinghouse and Asea Brown-Boveri Corporation (ABB). The plants went into commercial operation in 1968 and 1972, respectively. In 1989, NOK decided to replace the original Westinghouse P-250 plant computer with a modern distributed computer network and extended the functionality to what amounted to a control room upgrade. The project was known as the ANlage (plant) Information System (ANIS). ANIS provides process control data throughout the plant site, including the main control room, the emergency control room, the administration building, etc. In addition to the usual plant computer functions of real-time data logging and some process data analysis, the ANIS includes a fully computerized alarm system, a computerized procedure system that contains the Westinghouse Owners' Group Emergency Operating Procedures, and a modern computerized real-time data graphical presentation system.

The NOK ANIS architecture is based on the WDPF. For the ANIS application, NOK upgraded the WDPF by replacing the industrial version of the WDPF architecture with SUN Microsystems' SPARC UNIX-based servers and workstations. Subsequently, this became the standard

product configuration. The WDPF communications backbone was retained. Two sets of WDPF networks are employed in the ANIS design. One carries the process data from sensors to computational nodes (i.e., servers) and to a historical storage and retrieval system. The WDPF data networks are redundant by design.

NOK also added a third set of Ethernet networks that are dedicated to the needs of the alarm system. This was done to ensure that possible time delays due to heavy loading/data traffic on the system network would not interfere with the time response of the abnormality messages appearing on the various alarm system display devices.

The ANIS software structure is a set of monolithic computational systems that are connected by a WDPF data network to have access to the same real-time process data. In the ANIS software architecture, there is little attempt to share calculated results. This is the result of the use of "legacy" software and a communications network technology (state-of-the-art at the time of design), which is close to its reliability limits without this additional communications burden. Essentially, these systems listen for new process data, perform their calculations, and make the results available for display.

The ANIS hardware design was modeled by the Westinghouse Electronic Systems Reliability Group using component manufacturer's statistics for mean-time-before-failure and mean-time-to-repair assuming that adequate inventories of replacement parts were on location at the Beznau site. The resulting analysis demonstrated that the hardware architecture for the alarm system and the computer-based procedure system met or exceeded the design goal of 99.9-percent availability. Not all of the other computational nodes are redundant, so the reliability of data from those nodes was lower.

The ANIS design uses two types of data networks, including the WDPF data highway and the industry-standard Ethernet data network. The WDPF data highway is a proprietary design that is optimized to efficiently communicate real-time fixed-format data records, called "points." To do this, the WPDF data network uses a synchronous broadcast technique with fixed time slots that guarantee delivery time. This technique places an absolute limit on the number of points that can be transmitted on the network. Other than the point data, there is little management of data. In other words, the ANIS is a set of monolithic computational subsystems connected by a WDPF data network that collects plant process data. There is little that is communicated between these individual subsystems about the results.

Because of network loading concerns, abnormality messages that appear on the advanced alarm system are not available through the communications network for use on the displays or for a stimulus to the procedures. Conversely, some complex process data analysis applications can only provide their results for display, but are not available for use in building abnormality message logic or for use in the computerized procedures. The original WDPF design captured the real-time database only on the WDPF data highway. By contrast, as part of the ANIS design, a computational node also captures the real-time database . Application software is maintained on a network server that downloads requested software to servers and workstations on the network. This is a "by request" operation and represents a significant data load on the Ethernet networks.

Some application programs, specifically the advanced alarm system and the computerized procedure system, are systematically separated from the plant-specific database in the online

software that processes that database. This separation is analogous to the notion developed in the artificial intelligence work of the 1980s (i.e., separate the "knowledge base" from the "inference engine"). In such plant-specific databases reside the data processing algorithms/logic, constants and coefficients, rules for prioritization of display and processing, and instructions for data display creation.

Other applications provide the plant-specific data in the processing software. Clearly, this mixed set of approaches to databases and software provides for some interesting approaches to the initial verification and validation (V&V) effort and the processes of life cycle configuration management.

One concern with employing a distributed network for use in real-time process data analysis, control, and display is that of data coherence. Under steady-state conditions, the data can be considered consistent or coherent, but under transient conditions, the validity becomes much less clear. Timing of data is a difficult issue to assess and control in a distributed computer network.

The ANIS system was subjected to numerous tests of various levels of system completeness and function. The most robust tests were the factory acceptance tests conducted as a final system test at the Westinghouse manufacturing site before shipping the system to the Beznau site. This test was an exhaustive integrated system test, which tested the hardware as a connected system and the hardware/software as an integrated system.

2.2.3 N4 Series

In the late 1970s, the French nuclear power industry undertook the design of a very large (1,500-MWe) PWR. The N4 was the first to use the numerical integrated protection system (SPIN) technology, which was the most modern computer technology used in French safety systems at the time. The French also included a radical new design for the I&C and human-system interface. The main control room operator stations are compact cockpit-style, sit-down workstations that are entirely driven by digital computers. Graphical visual display units (VDUs) display process data, plant graphics, procedures, and alarms; touch screens provide the means of executing manual controls. The entire I&C architecture was, for the first time, to be based upon the use of digital computers, rather than analog hardware.

The I&C system architecture of the N4 is conceptualized in four levels. Level 3 is the human-system interface processing level; Level 2 is the processing and communications level; Level 1 is the data acquisition, signal processing, and control level; and Level 0 is the process level. Level 3 includes the control room system which are composed of mainframe computers manufactured by Thompson-CSF, at least on the Chooz B version of the N4. At Chooz B the control room hardware is a late 1970s vintage design using late 1970s computer technology. Level 2 provides immediate support to the operator under normal, incidental, or accident conditions. These functions require the management of a large amount of process and calculated data that is transmitted for display, logging, and analysis. The generation of additional calculated data through application programs includes core mapping, fuel burnup, load following, xenon following, and equipment monitoring. Storage and retrieval of historical data for post-event analysis are also available. Data processing needed to support plant operation and supervision is distributed through level 1 and consists of the following tasks:

- time tagging and validation of raw process data
- monitoring of process parameters of automatic actions initiated by the control system
- detection of deviations from normal or required states and, therefore, generation of alarms concerning critical functions, violation of technical specifications, and unavailability of essential or important functions
- filtering of alarms depending on plant mode
- grouping of alarms to account for process redundancies and functionalities
- integration of the different parameters to provide the system manager with a general view of the unit status and dynamic behavior

Level 1 includes the protection and control functions. The implementation of the automatic protection functions is preformed by SPIN, which includes some associated systems such as the control rod drive system. SPIN has the high reliability typical of a four-way redundant system. The N4 plant has four trains of safety features equipment. The control system has a reliability typical of a modern distributed industrial digital control system. However, human-system interface processing and communications may lack the robustness of modern distributed computer systems.

The N4 I&C architecture comprises several major systems from different vendors, each of which has a different methodology and different level of automation for managing data. Consequently, the data must be arranged at interfaces between the systems to fit the format required by the data user.

The Chooz B N4 computer technology used for Levels 3 and 2 uses mainframe computers and the Fortran programming language. On later versions, it is believed that Electricite de France (EdF) will change this portion of the architecture to a UNIX-based workstation client-server network.

One of the more innovative parts of the N4 I&C design is the set of support tools that EdF has built to support the design. First, EdF has completely computerized all of the design data about the N4. This includes the piping and instrumentation diagrams (P&IDs), systems descriptions, procedures, control logic, electrical one-line diagrams, etc. In the late 1970s and early 1980s, EdF installed this data in a relational database management system called PHENIX, which was originally developed by the British to aid in the design of piping layouts. EdF adapted this database management system to their purposes of supporting the I&C design and configuration management effort for the N4 plant design. EdF also built a database of control room display objects (macros) in another relational database management system called SOCRAT and interfaced it with PHENIX. This coupling has enabled EdF engineers to build code by making VDU screens on workstations in their engineering offices that can be directly compiled on the N4 I&C at the plant site. The database management systems can build the appropriate links to process parameters and synthetic variable calculations within the N4's online database, and automatically produce the requisite software based upon screens that engineers build on workstations.

2.2.4 Swedish BWRs

The Swedish nuclear industry has undertaken an aggressive modernization program. Specifically, the Swedish nuclear industry has a consensus agreement that modernization of I&C systems can have a positive impact on plant safety. The first I&C modernization project was the Oskarshamn 1 BWR I&C system upgrade based on the ABB Advant Open Control System (AOCS) distributed digital control product.

The AOCS data communications network in the Oskarshamn 1 I&C system has three levels, including the corporate/business network, the control network, and the sensor bus. It also usestwo controller types, including the Advant Controller 160 (AC160) and the Advant Controller 450 (AC450). The AC160 (developed by ABB of Manhiem Germany) is used for the safety functions, while the AC450 (developed by ABB of Sweden) is used for non-safety control functions. To meet the various environmental and seismic requirements of various countries, there are three different versions of the AC160 racks, each specific for the Swiss, U.S. and Korean markets. The AC160 and AC450 controllers use different hardware and software operating systems, yet both are programmed using the same graphical programming language. This provides a balance between achieving equipment diversity and facilitating plant personnel familiarization.

The protection system has the high reliability associated with a two-out-of-four trip system logic design. Redundancy is included in each division of safety equipment using multiprocessing. However, the AC160 multiprocessing redundancy shares some common resources, such as the computer bus. The AC450 control system controllers can be configured with redundant microcomputer modules but the microcomputers share common computer and input/output (I/O) resources.

The AOCS uses the Advant Series 500 Operator Stations for its human-machine interfaces (HMIs). The Advant Series 500 Operator Station and the associated data management systems, such as the data storage and retrieval system, provide the operators with supervisory and control interfaces. The Series 500 Operator Stations can be applied as multiple copies in physical or parallel redundant configurations. However, some of the plant process data management stations, such as the data storage and retrieval unit, are not redundant.

Networks, such as the MB300 control network used in Oskarshamn, are not usually based on Ethernet because of inherent limitations in the Ethernet architecture. The AF100 data transmission rate of 1.5 Mbit/second is typical for a remote I/O function, but may be too slow for communication between controllers. The two control networks, MB300 and AF100, use different approaches for the transmission of plant process data. The AF100 uses a continuous cyclic update method for the transmission, while the MB300 holds the plant process data locally and transmits only upon request. It is unusual to have two different control network approaches for similar functions within the same architecture.

The Advant Series 500 Operator Stations, MB300 control network, and AC450 transmitter concept for acquisition of plant process data can be efficient for some system configurations. The AF100 control concept offers some amount of determinism in data communication. The plant network and control network are 1980s technology, so it is likely that they will be upgraded in the near future.

2.2.5 Temelin

The VVER-1000 nuclear power plants located at Temelin (in the Czech Republic) provide another example of a PWR I&C upgrade project. The Czech Republic decided to install Westinghouse I&C in these plants. Temelin underwent extensive instrumentation, control, and safety system upgrades using Westinghouse technology.

The Czech Republic chose the Central Electricity Generating Board (CEGB), now British Energy (BE), owner and operator of the Sizewell B plant as a consultant to aid in writing the specifications for the new I&C system. The Czechs enhanced the Sizewell B style design framework with three additional high-level requirements. Automation was to be significantly increased in comparison with Sizewell B. The new I&C systems were added to Temelin as a diverse system to the originally installed Russian-designed systems.

The first additional requirement was to provide a system that allows operators to start the reactor from cold shutdown to hot zero power with the push of a button. This represents a large step beyond current European automation, which typically has the capability to automatically startup the steam side or balance-of-plant (BOP) side of the plant.

The second additional design requirement provided for the installation of Westinghouse process sensors, such as resistance temperature detectors. These sensors were installed according to the Russian design (i.e., each of the three Safety Class 1E instrument channels in the reactor system would be triply redundant). The Russian design has this level of redundancy because of the lack of reliability of Russian-built sensors. The second requirement also provided for the installation of modern sit-down control boards at each unit, which are backed up by an analog-style control board with discrete controls and displays.

The third additional design requirement provided for a diverse protection system. It also provided for a "limitation" system that functionally operates between the control system and the protection system.

At Temelin, core protection is provided by the Primary Reactor Protection System (PRPS) and the Diverse Protections System (DPS). The PRPS performs all of the automatic functions required for reactor trip and emergency safety features and provides a control path for the manual actuation of the safety components. The PRPS consists of three divisions. Each division provides measurement, processing, and actuation functions. Triple redundancy facilitates two-out-of-three voting for reactor trip and automatic safety feature actuation.

Two-out-of-three voting logic meets the single-failure criteria, where it is arbitrarily assumed that one channel may fail and another channel may be undergoing maintenance. However, in the reduced one-out-of-two configuration, the system is vulnerable to spurious actuation. Consequently, the Czechs added extra microcomputer subsystems to the design to ameliorate the situation by providing spare internal redundancy within a division used during maintenance and testing.

The reliability of the PRPS with respect to component failures was estimated to be 10^{-5} failures per demand. However, the failure to trip is considered limited by common-mode considerations rather than random failures. To meet the goals of the safety case, the Czechs added a second,

diverse protection system, called the DPS. A key design requirement imposed on the PRPS and the DPS is that the overall plant protection system must be capable of mitigating "frequent events" concurrent with a postulated common-mode failure in either the PRPS or DPS, but not both simultaneously.

2.2.6 Advanced Boiling-Water Reactors (ABWRs)

In 1978, General Electric (GE) began the conceptual design of a family of advanced light-water reactor plants that share a common technology base. These are the 1,300-MWe ABWR and 600-MWe Simplified Boiling-Water Reactor (SBWR). The world's first ABWR, Kashiwazaki-Kariwa Unit 6, was completed in Japan by a consortium of Toshiba Corporation, Hitachi Ltd., and GE. This was followed by Kashiwazaki-Kariwa Unit 7. The design of these two units is similar to ABWR designs certified by the NRC. Commercially operated by Tokyo Electric Power Corporation in the Niigata Prefecture. Kashiwazaki-Kariwa Unit 6 began generating electricity in December 1996 and Kashiwazaki-Kariwa Unit 7 began commercial operation in July 1997. A third ABWR in Japan, Hamaoka Unit 5, is scheduled to be completed in 2004.

The Kashiwazaki-Kariwa plants in Japan were the ABWRs reviewed in this study. The I&C systems use state-of-the-art digital and fiber optic technologies. The ABWR has four separate divisions of safety system logic and control (SSLC), including four redundant multiplexing networks to ensure plant safety. Separate control rooms and other panels house the SSLC equipment for controlling the various safety function actuation devices. The diverse I&C features are designed to provide protection against common-mode failures of the protection systems.

Reactor trip process variables are acquired by a remote multiplexing unit (RMU), which converts the signals into a format suitable for multiplexing. The data from each RMU are converted into optical signals and sent via an optical network to corresponding digital trip modules (DTMs) within the associated SSLC device. The DTMs perform the trip logic calculations by comparing the individual monitored variables for a given division with set point values and, for each variable, send a separate "trip" or "no trip" signal to the trip logic unit (TLU) in that division, and to each TLU of the other three divisions. Communication with the other three divisional TLUs is via fiber optic serial data links. The DTMs and TLUs use separate microprocessors. The software in these processors does not perform any other safety-related logic functions.

Two-out-of-four voting is performed by the TLU, and this trip information is sent to the output logic unit (OLU), which sends a trip signal to trip actuators. The OLU enables the TLU in the associated division to be bypassed. That is, it sends a trip output to the load drivers when the associated division is bypassed.

Each system includes microprocessors to process incoming sensor information and to generate outgoing control signals, local and remote multiplexing units for data transmission, and a network of fiber optic cables. The controllers are "fault tolerant," meaning that they continually generate signals to simulate input data and compare the result against the expected outcome. Controllers for both sensors and equipment are located on cards that are remotely distributed. If the controller detects a problem, a signal is sent to the control room. The malfunctioning card can be replaced with a spare card within a relatively short time.

2.2.7 CANDU

In CANDU reactors, computerized control systems and fuel handling control systems were introduced in the 1960s. The current CANDU 6 plant design has evolved over the past two decades based on the design developed in the 1970s for the original CANDU 6 plants at Point Lepreau and Gentilly in Canada, Wolsong in Korea, and Embalse in Argentina. The most recent deployment is for the Quinshan plant being constructed in China. Changes and additions to the CANDU 6 design have been made over time to reflect experiences in Canada and elsewhere. The design evolution is expected to continue for the foreseeable future with potential inputs from all current generation CANDU plants and the Advanced CANDU Reactor (ACR-700). The Darlington four-unit nuclear power station, which went on line in 1990, was the first CANDU plant to use fully computerized shutdown systems. The licensing of the Darlington station in the late 1980s included an extensive review of the shutdown system software.

The CANDU architecture is divided into seven physical plant areas, including the main control room (MCR), two control equipment rooms, computer room, auxiliary computer room, work control room, and technical support center. The MCR contains the nuclear steam supply system (NSSS) and BOP main control panels. The control room instrumentation is based on the philosophy of having sufficient information displayed to allow the station to be controlled safely from the control room. To achieve this goal, all indications and controls that are essential for operation (i.e., startup, shutdown, and normal operation) are located in the MCR panels. The equipment panels containing the reactor regulating system equipment for the shutdown of the reactor and the activation of safety equipment are seismically qualified. The remainder of the panels, including the main control panels and the digital control computers (DCCs) are not seismically qualified. However, the "watchdog timer" portion of the DCC, which is an independent hardware device that monitors the operation of the DCC, is seismically qualified for a design-basis event.

The unit DCCs and support subsystems are located in the computer room of the control equipment room. The computer room is completely enclosed and has its own heating and air conditioning systems. This ensures a relatively dust- and dirt-free environment. The maintenance computer DCC is located in an adjoining room (i.e., the auxiliary computer room).

As part of the safety analysis for Canadian nuclear power plants, a qualitative reliability analysis is required. For the digital protection systems, reliability qualification (a testing technique based on statistical observations) is used to estimate the probability that the software will fail to meet its functional requirements. Eight thousand test cases were run for each shutdown system software.

2.3 Future Advanced Reactor I&C Designs

2.3.1 Advanced Plant (AP)-600/1000

Two other I&C designs reviewed in this report are the Westinghouses AP600/1000 advanced reactor designs. These designs are the result of a Westinghouse-led industry effort to design and obtain early regulatory approval of a PWR plant design that embodies the lessons learned from the previous 40 years of nuclear power plant operations. The U.S. nuclear industry captured much of this experience in the Electric Power Research Institute (EPRI) Advanced Light-Water Reactor (ALWR) Utility Requirements Document. In designing the AP600/1000 design, Westinghouse sought to meet, or exceed, those requirements.

The Westinghouse AP600/1000 I&C designs are based on the following principles:

- The architecture will distribute elements closer to the monitor systems and parameters.
- The architecture will be consolidated by function into an efficient size and layout.
- The latest industry and regulatory requirements for safe, reliable, and efficient plant operation will be addressed.
- Separation between non-safety and safety systems will be maintained.
- Systems will use redundancy to meet high reliability and availability goals.
- The design will enhance and simplify maintenance and testing.
- The systems will be integrated such that data and information are handled consistently.
- Industry-standard open interfaces will be provided for third-party equipment.
- Data transfer between the I&C network and the station information system will be provided.

Various types of redundancy are employed throughout the system architecture to yield a fault-tolerant design. Specifically, the types of redundancy employed include physical (or parallel) redundancy, channel sets, trains, and workstations. Active and standby redundancy is employed in controllers and workstations, and communication connection redundancy is employed in network concentrators, controllers, remote I/O, and workstations. Process interface level redundancy for critical systems is employed for both analog and digital inputs and outputs, as well as power supplies.

Information and data management requires efficient data sharing among the HMI elements. In addition, the system will be integrated such that data and information are handled consistently across the system. The requirements for information and data management necessitate high-performance microcomputer and data highway technologies.

Main control room dynamic proof of concept testing was performed by Westinghouse using a mockup and test facility that was driven by a nuclear power plant simulator. There is a primary focus on human factors testing using experienced operators. Westinghouse will perform full-system validation testing prior to equipment installation.

2.3.2 Advanced Pressurized-Water Reactor (APWR)

The Advanced Pressurized-Water Reactor (APWR) is a large four-loop nuclear power plant designed jointly by the Westinghouse Electric Company (WELCO) and Mitsubishi Heavy Industries, Ltd. (MHI) of Japan. The design is scheduled for application in Japan in the near future. Mitsubishi Electric Company (MELCO) will supply the APWR instrumentation, protection, control, and control room equipment. MHI and MELCO are in the same company family but operate separately. MELCO is the oldest licensee of the former Westinghouse Electric Corporation. Under a supplement to this license, MELCO obtained detailed design information for the Westinghouse IPS, ICS, and Black Board artificial intelligence technologies. In addition, MELCO participated with Westinghouse Electric Corporation in the development programs. Westinghouse also assisted MELCO with APWR control room design by performing certain development and verification activities.

The APWR I&C architecture is similar to that of the the AP600 advanced reactor. However, there are differences in the design details, especially in the MCR. The reactor reactivity and operation control, or NSSS control, is patterned closely after the Westinghouse ICS. The design of hardware modules and system software is in common with the digital protection system. The BOP, including the turbine control, is controlled by an extension of the digital control system, which has a dedicated data highway network.

The design and V&V methodology follows nuclear industry standards with an emphasis on testing. Hardware elements are methodically tested. Extensive system validation testing is relied upon to demonstrate proper system operation. Main control room dynamic proof-of-concept testing was performed using a mockup and test facility that was driven by a nuclear power plant simulator. Some tests were performed using experienced operators.

Pre-production protection and control systems were tested as complete systems. However, this was several years ago and it is the designers' intention to build the APWR plant systems using a new hardware design. Therefore, significant factory testing of the APWR plant systems will be required.

2.3.3 High-Temperature Gas Reactors

The GT-MHR and PBMR designs combine features that lead to high thermal efficiencies, cycle simplicity, enhanced safety, and improved economics. A very high level of automation will be designed into the GT-MHR and PBMR plant control systems based on economic, reliability, and operability requirements. Some control system designs will come from current industry experience with automation for multi-module plants, including steam and gas combined cycle plants in the United States and Japan. However most of the instrumentation, control, and protection system designs will need to be developed before these new plants can be licensed and built.

2.3.3.1 Pebble Bed Modular Reactor

A significant digital I&C system planned for the PBMR is the automation system (AS), which will perform power plant monitoring, control, and protection functions. The AS hardware design will use integrated commercial off-the-shelf (COTS), all-digital programmable systems. The AS will consist of several subsystems, including the reactor protection system (RPS), post-event instrumentation, equipment protection system, operational control system (OCS), and human-system interfaces (HSIs).

The safety system designs will comply with the IEEE standards and NRC guidance applicable to the PBMR design. Digital platforms will be used for safety systems; therefore, adequate diversity and redundancy will be required. Current design concepts contain specific provisions to address common-mode failure. This includes RPS functions that are also duplicated in the non-safety OCS (which is a platform diverse from the RPS) and contain provisions for manual initiation of a reactor trip.

The plant control data and instrumentation system (PCDIS) will use industrial, distributed microprocessor-based control platforms. The PCDIS will be a hierarchical data information network that is functionally separate from and physically independent of the Class 1E nuclear safety systems and the human-factored operator interfaces. The plant control system will integrate major plant instrumentation systems using highly reliable, multiple-redundant data networks with fiber optic isolation. Control signals and data gathered from sensors will be communicated via remote field control stations located throughout the plant. Redundant data networks will connect these remote stations with the main control computers and the control room. The integrated PCDIS will provide plant operators real-time plant status information.

The PCDIS will regulate and coordinate the operation of plant systems through feedforward and feedback algorithms. The transparency of the helium primary coolant to the neutron flux, the absence of boiling and phase changes in the cooling system, and the large thermal capacity of the graphite-moderated core enable the PBMR to have a relatively long, stable, and predictable time of response. The control strategy for the PBMR is designed to take advantage of these inherent characteristics.

Previous studies regarding operation of multiple-reactor modules led to selection of a single control room. This configuration provides a separate workstation for each module, plus an additional workstation for common plant auxiliary systems. The PCDIS design concept is driven by top-level operations and control requirements, including human factors; reliability and availability requirements; and interface requirements with the nuclear, fluid, mechanical, and electrical systems. It has the following key design features:

- The single control room design will have a separate operator workstation for each reactor module, plus a workstation for common plant auxiliary systems.
- Dedication to plant control and instrumentation functions with no interaction with the safety-related protection system functions.
- Distributed control functions will be handled by control processors located near the plant systems they control.

- Proven microprocessor-based distributed control systems will connect control room operator interfaces and local control processors via redundant data networks. The system is hierarchically arranged to limit failure effects and to provide high response speed; high reliability; and high security for local control, module monitoring, production plant monitoring, and PBMR complex monitoring.
- Advanced HMIs will incorporate real-time animated graphic displays, touch-sensitive screens, color graphics, and audible output messages to enhance operator effectiveness.
- High levels of redundancy for controlling nuclear power and heat removal systems will be designed to meet or exceed reliability goals with high assurance and to minimize challenges to protection systems.
- A highly automated control scheme will provide the operator with the means for manual intervention at all times.

A central technical management information system and technical database, with plant design, test, and maintenance data, will be provided to support technical personnel.

The design will also support the idea of distributing process information and online monitoring information to different personnel (plant manager, maintenance manager, chief engineer, etc.) who have an interest in plant and system status. Plant operational information will be available on the plant intranet for access by designated persons. No control actions will be performed from computers on the network.

2.3.3.2 Gas Turbine Modular Helium Reactor

The plant protection and instrumentation system (PPIS) for the GT-MHR will comprise three subsystems, including safety protection, special nuclear area instrumentation, and investment protection. The PPIS design will have reactor trip, main loop shutdown, and initiation of the shutdown cooling system functions. In addition, the PPIS design will meet the requirements of Title 10, Part 100, of the *Code of Federal Regulations* (10 CFR Part 100). The hardware portion of the PPIS that accomplishes these functions will be grouped and labeled as the safety protection subsystem. The PPIS hardware that will provide the other active functions will be grouped and labeled as investment protection subsystems.

Each reactor module will have a separate and independent safety protection subsystem that will consist of four separate (redundant) safety channels with two-out-of-four coincidence logic to command initiation of a reactor or turbine trip. Each safety channel will include the field-mounted process variable sensors, electronic signal conditioning equipment, and electronic trip setpoint comparators to provide a trip signal when the process variable reaches the trip setpoint.

The GT-MHR will also use an OCS that will be an industrial-grade distributed control system with redundancy for certain functions to enhance availability. It comprises controllers and remote I/O modules distributed throughout the plant. Data exchange between the remote I/O, controllers, and other intelligent field devices (e.g., smart valve positioners) will be via fieldbus digital networks. The OCS's main function will be to control power generation of the plant. The plant support systems (e.g., compressed air, waste handling) will be controlled by dedicated "small" control systems that operate independently of the OCS; however, essential

information will be displayed on the OCS, and data will be captured on the data server. These controllers will be connected to the redundant OCS (industrial Ethernet) optical networks. The OCS software will be organized in a hierarchy of super and subordinate group controllers to execute the OCS functions in a structured manner. The group controller structure will be organized in three tiers, making provision for sequential control, continuous control, and calculations and monitoring functions.

Besides the control of power generation, the OCS will also execute a backup RPS function (diverse platform). It will also perform limitation actions by steering the reactor away from possible trip condition by providing "run-back" (i.e., reduce power rather than tripping the reactor).

3. DESIGN, APPLICATION, AND PERFORMANCE EXPERIENCE

This section focuses on unique characteristics of advanced technology or technical methods that have contributed to the success or failure of particular applications. Limited performance experience from evolutionary nuclear power plants also is presented. Following a brief discussion describing the sources of information that were reviewed, this section describes other countries' experiences with the phased introduction of digital technologies; diversity and defense-in-depth design approaches; software tools and configuration control; software V&V; software errors; and hardware failures.

3.1 Sources of Information

Digital I&C technology has seen widespread use in non-nuclear applications within the international industrial community. The use of digital technologies has increased for both non-safety and safety-related applications in the nuclear industry, such as at the evolutionary plants that are the subject of this study. In addition, current ALWR designs and next-generation reactor concepts incorporate extensive use of advanced I&C technologies. The expanding experience with advanced I&C technologies should provide a wealth of information regarding implementation issues and performance characteristics that should be considered in evaluating advanced technologies for application in safety-related I&C systems at nuclear power plants.

Many resources were examined in this study, such as technical journals, conference proceedings, event reports maintained by regulatory bodies, and industry-maintained operational databases. Significant information was gained from topical conferences and workshops that have been held over the past decade. In particular, useful information resources have included the series of American Nuclear Society Topical Meetings on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies; the annual Power Plant Dynamics, Control, and Testing Symposium; the Organization for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA) Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, the International Symposium on Future I&C for Nuclear Power Plants; and selected EPRI workshops.

The information available from operational, performance, and reliability databases was limited by availability and access. The NRC's Licensee Event Report database is the most accessible and has been extensively reviewed for I&C failure information. Other databases considered in this study included the Institute of Nuclear Power Operations (INPO) Equipment Performance and Information Exchange (EPIX) database, the OECD/NEA Computer-Based Systems Important to Safety (COMPSYS) database, the Central Research Institute for the Electric Power Industry (CRIEPI), Nuclear Information Center (NIC) Nuclear Component Reliability Data System, and electronic component reliability data maintained by the Reliability Analysis Center (RAC) in Rome, New York. Because of the absence of extensive performance databases for digital equipment and the product-specific nature of the information that was available, this section focuses on reported experience from individual applications of advanced I&C technology at the evolutionary plants that are the primary subjects of this study. Such experience can be categorized in terms of system design and implementation approaches, software quality and performance, and hardware failures.

3.2 Phased Introduction of Digital Technology

Japan

Microprocessors have been used in Japanese nuclear power plants for more than 30 years. The Japanese nuclear power industry, in collaboration with the Ministry of International Trade and Industry (MITI), evolved from analog to digital I&C technology in an orderly, step-wise fashion. From the early 1970s through the mid-1980s, computers and microprocessors were used primarily for information processing and display of results. In the 1980s, digital technologies were integrated into the control systems for various subsystems, starting with auxiliary systems and then moving to principal control loops. By the 1990s, microprocessors were being used for data logging, control, and display for most non-safety-related systems. The first fully digitalized I&C system was integrated into the Kashiwazaki-Kariwa ABWR in 1996.

As part of the evolution toward the use of microprocessors in safety-related applications, a national program was established involving regulators, researchers, and manufacturers. Reliability testing of software used in safety protection systems began with individual safety-related systems in the mid-1980s and progressed to the safety protection system by the early 1990s. For the national qualification program, functional tests were performed on one complete train of digital safety system equipment, with inputs from remaining logic trains simulated by computer inputs. Using noise superimposed onto test signals, these functional tests also were conducted with instrumentation subjected to simulated conditions of aging, seismic disturbances, and accident environments. The process for accomplishing these tests involved verification followed by validation (i.e., "proving" tests). The verification process consisted of the following steps:

- clarification of the functional and performance requirements for the test devices, based on regulations and test device specifications
- confirmation that test device specifications were consistent with regulatory requirements
- determination that specific test conditions were based on device specifications and expected plant conditions
- documentation of test procedures

Validation test procedures were consistent with those specified by IEEE Std. 323-1974 for Class 1E electrical equipment at nuclear power plants, which included both electrical tests and the following safety function tests:

- input/output tests
- automatic system initiation
- manual operation
- bypass functional tests on individual sensors and complete channels

As an integral part of these tests, equipment was subjected to the following conditions:

- sensor failure
- noise
- various ambient temperatures

- thermal aging
- simulated seismic conditions

The coordinated, systematic introduction of digital technology into Japanese nuclear power plants has been effective. The experience gained from non-safety-related applications, coupled with the confidence derived from the Japanese national qualification program, permitted an orderly transition to digital I&C systems while the supporting infrastructure was developed concurrently.

3.3 Diversity and Defense-in-Depth Design Approaches

Korea

The use of digital technologies in the Republic of Korea began in the late 1980s through the use of microprocessor-based I&C equipment in the safety-related Digital Interposing Logic System (DILS) at Yonggwang (YGN) Nuclear Power Station Units 3 and 4. The NSSS protection signal processing and bistable circuitry were upgraded at Kori Nuclear Power Station Unit 1 using commercial-grade digital process instrumentation. Uljin Nuclear Power Station Units 3 and 4 employ microprocessors for plant control systems, including additional logic between system- and component-level circuits. These non-safety-related control systems are based on programmable logic controllers (PLCs). All of the protection systems, including the reactor trip system and engineered safety features actuation system (ESFAS), of Uljin Nuclear Power Station Units 5 and 6, are being built to use digital technologies, but the MCR and the remote shutdown panels are still based on conventional technologies.

With the introduction of digital technology into safety systems at nuclear power plants, Korea Institute of Nuclear Safety (KINS) has placed special emphasis on diversity and quality as principal factors in addressing the potential for common-cause failures. At YGN Units 3 and 4, the DILS is an integrated microprocessor-based control system that receives actuation commands from the control modules mounted on control panels, on/off logic actuators, and other control systems. The DILS also sends the output signals to field devices. Each DILS control board has its own dedicated control card, I/O buffer cards, and I/O terminations. However, because common-mode software programming errors remain possible, KINS required a diverse backup system. To meet this requirement, a set of safety-grade, hardwired displays and controls were installed on a backup panel in the MCR to allow manual actuation of ESFAS train B equipment.

KINS addressed the issues of diversity and software quality during its design review of Uljin Units 5 and 6, which are currently under construction. For these units, the digital plant control system (DPCS) will fulfill the same function as the DILS for the YGN units. In addition, the Uljin units will have digital plant protection systems (DPPSs), which include the reactor trip system and ESFAS. Thus, digital technology is being employed at both the system and component levels. The review of the Uljin Units 5 and 6 design found that the system and component-level circuitry are diverse because they use different technologies and vendors. Thus, KINS concluded that little likelihood existed for common-cause failure affecting both levels. However, to provide protection against common-cause failures within each level, two kinds of backup panels have been required in the MCR.

A backup system at the system level was added against loss of the DPPS due to common-cause failures. This backup system is totally diverse from the DPPS and the system designed to backup DPPS during anticipated transient without scram (ATWS) events. Thus, three layers of independent and diverse defense-in-depth exist at the system level.

As with YGN Units 3 and 4 and Uljin Units 3 and 4, KINS required a backup panel at the component level. This panel is independent and diverse from the system-level backup and the DPCS, so there are two component-level layers of defense-in-depth.

KINS required the installation of redundant microprocessors in each channel to increase the availability, testability, and reliability of the DPPS. As a result, two microprocessors are used for the bistable function and four microprocessors for the local coincidence logic function. This architecture can provide physical redundancy, but can also support software and functional diversity within each channel. As an additional measure to address software common-cause failure, KINS required third-party review independent of the software design, as well as verification teams to enhance the software quality and reliability of the DPPS for Uljin Units 5 and 6.

The reactor protection system and plant control system at the Kori Unit were upgraded as a result of component obsolescence, high maintenance costs, and concerns about aging. The upgrades were implemented using the Foxboro Spec 200 (analog) and Foxboro Spec 200 Micro (digital) line of process instrumentation. A defense-in-depth and diversity assessment was performed using the licensed design bases for plant responses to conditions and transients. This assessment determined that common-cause vulnerabilities existed in the reactor protection system. To address these vulnerabilities, the Spec 200 Micro modules for process parameters (such as for pressurizer pressure, steam-generator water level, and containment pressure) were replaced with Spec 200 analog modules.

During the design certification review of the Korean Next-Generation Reactor (KNGR), KINS raised issues regarding the system structure of the advanced DPPS design, the safety classification of soft controllers introduced in the DPPS, and the defense-in-depth against common-cause failures. The integration of the bistable and local coincidence logic functions into a common microprocessor caused concern. Previous designs that had been licensed implemented these functions (the generation of trip signals and coincidence logic signals) on physically separate microprocessors. The integrated structure caused concern about reliability, functional diversity, and design consistency of the more complex software. To address these concerns, KINS is requiring that separate bistable and local coincidence logic microprocessors be maintained in the design to preserve functional distribution and to facilitate software V&V.

The next issue addressed in the KNGR design certification involved the safety classification and independence of the soft controller to be installed in the digital ESFAS. The I&C systems of KNGR are designed using digital technologies like multiplexers/demultiplexers in safety systems to process data efficiently and to design compact and efficient systems. Thus, soft controllers replace a large number of spatially distributed manual switches. Two concerns were that this design change makes it more difficult to ensure the independence between safety and non-safety signals and increases the software V&V effort. Because manual switches that are used to control the safety-related components are classified as part of the safety system, KINS adopted the position that soft controllers that are functionally equivalent to manual switches will

also be classified as part of the safety system, including both software and hardware. In addition, the electrical isolation and physical separation among channels will be maintained.

3.4 Software Tools and Configuration Control

United Kingdom

British Energy, Plc., the owner-operaror of the Sizewell B nuclear power plant, created an offline database to define the Sizewell B ISCO design. The database is supplemented with graphical depictions of control logics and MCR mimics. Graphical depictions are objects instantiated by fields in the database. The database was an effective configuration management tool for a very large control and supervisory system.

For Sizewell B, the software verification analysis and testing of the IPS common microprocessor services code was aided and automated by a software tool. The "test-bed" tool was an adaptation of a PL/M-86 of a tool developed by Liverpool Data Research Associates to analyze Pascal software code. The test bed imposed formalism and objectivity to the independent assessment and testing process for each life cycle phase in which it was used. The test-bed tool was used to statically analyze the code to ensure that correct programming standards were followed and code complexity was controlled. The test bed tool was also used to establish the coverage of the dynamic test cases developed from the software analysis. The verification test cases were required to have 100-percent path coverage at the module level.

The software for the IPS and ICS was developed and is maintained using a set of mainframe computer software tools. The tool set includes a configuration management tool that, among other things, tracks all software changes. Proposed software changes must be agreed upon by a group of software experts who are knowledgeable of the IPS/ICS software design and verification. The software librarian is the only person authorized and able to change the code. The change control procedure requires change verification before application in a safety system.

The executable form of the software module also resides in the library. That is, modules do not require recompilation to be used in different subsystems or systems. Executable modules, along with subsystem configuration and calibration data, are linked and located in such a way as to form a memory image of the microprocessor software. The link location process includes the generation of a checksum from a mainframe calculation of the memory image. A separate checksum calculation is performed by the host microprocessor as part of the startup sequence. This ensures the integrity of the transfer process from the mainframe computer to the microcomputer. The checksum calculation is repeated throughout the microcomputer operation.

The change control and configuration management for the hardware follows corporate drafting standards used for previous generation protection systems. After installation, the executable code that has been burned into programmable read-only memory (PROM) was treated as hardware. The microprocessor printed circuit board is imprinted with a drawing number that defines, among other things, the software configuration. A serial number is also imprinted.

France

One of the more impressive parts of the N4 I&C design is the set of support tools that EdF has built to support the design. EdF has completely computerized all of the design data about the N4 plant. This includes P&IDs, system descriptions, procedures, control logic, and electrical one-line diagrams. In the late 1970s to the early 1980s, EdF installed this data in a relational database management system called PHENIX, which was developed by the British to aid in the design of piping layouts. EdF adapted this database management system to its purposes of supporting the I&C design and configuration management effort for the N4. EdF also built a database of control room display objects (often called "macros") in another relational database management system called SOCRAT and interfaced it with PHENIX. This coupling has enabled EdF engineers to build code by using engineering workstations to update VDU screens at the plant site. The database management systems can build the appropriate links to process parameters and synthetic variable calculations within the N4's online database, and the systems can automatically produce the requisite software based upon VDU screens. At the time of this study, the level and scope of automation was the most advanced compared to other nuclear I&C vendors.

Czech Republic

Westinghouse engineers created a very large offline database to define and control all aspects of the Temelin I&C upgrade design. The database used a robust relational database management system. For example, about 100 fields were used to define a sensor. The fields included information, such as the sensor supplier and qualification level, that were not incorporated into the online information system. One of the main benefits of such an approach was that various I&C engineering teams used a consistent data set throughout the upgrade project, and the data was associated with a level of certification and authentication. This database also allowed capture of design data provided by Czech and Russian plant designers, and it identified information that was missing early in the upgrade process.

3.5 Software Verification and Validation

United Kingdom

For the Sizewell B Nuclear Power Station, Westinghouse built a pre-production PPS for environmental qualification test purposes. After the completion of those tests, the unit was turned over to British Energy for use as a validation test unit. The pre-production unit was connected to a computerized test harness that performed a series of dynamic tests based, in large part, on the design-basis events. A subcontractor designed the test harness and executed the tests for British Energy.

Several of the dynamic PPS validation tests using the computerized test harness did not work. At first, these results were classified as test failures, implying problems with the PPS. However, British Energy engineers concluded that the PPS test harness contained timing problems. Those timing problems were resolved, and the tests were executed again with positive results.

France

EdF identified several unresolvable issues with the initial design for the control and protection system of the Chooz B Nuclear Power Station. The initial design was based on a unique architectural design. The initial Chooz B N4 plant I&C architectural design consisted of an automatic protection system and a decentralized control and monitoring system. The automatic protection system included the nuclear instrumentation, control rod controller, and reactor protection system (the SPIN system). The decentralized control and monitoring system included the CONTROBLOC P20 and the CENTRALOG P20 that were based on the Integrated System for Plant Operation concept.

CONTROBLOC P20 is a decentralized control system initially developed for the N4 plants by Cegelec. The purpose of the CONTROBLOC P20 control system was to provide plant control and a safeguard support system (Class 1E). The CENTRALOG P20 system was a supervision system to provide all plant computer functions and emergency response functions. The P20 system architecture was to be divided into distributed clusters consisting of a redundant bus network. The CONTRONET was to provide the control room network, the CONTROBUS was to provide the distributed control network, and the LOCABUS was to provide the field bus network. The computational platforms selected for the P20 systems included the Motorola 68020 microprocessor and INMOS transputer, which is a 32-bit microprocessor primarily designed for parallel applications (i.e., parallel processing). The configuration of the P20 system was to be based on an object-oriented design database approach using the CONTROCAD computer-based software design tool.

The unique features of the P20 system included the integration of Class 1E and non-Class 1E functions within a common architecture utilizing shared data paths. It also included the use of state-of-the-technology computing platforms, which had not previously been employed in nuclear plant applications and which did not have extensive performance histories. In addition, it included the development and application of a new design tool as the basis for system-wide software implementation.

The Chooz B N4 plant was originally scheduled to go into commercial operation in 1991 or early 1992, but the French regulatory authority interrupted the schedule because of its concerns about the P20 system. In particular, three main issues were identified:

- With its complex, fully redundant communication links and shared communication links between safety and non-safety functions, the P20 architectural design was extremely ambitious in light of the available technology. It was found that a communications-by-exception approach employed for some parameters created the potential for communication saturation of cluster interfaces (i.e., "choke" points) during off-normal events. While this response characteristic might have been addressed through design modification, the regulatory authority was concerned that the Class 1E functions could not be qualified without major design changes.
- Another issue was that the parallel development of hardware and software posed uncertainties about the ability to achieve expected performance. In particular, the transputers had never been used before, and the CONTROCAD design tool was unproven. As a result, the capability of the suppliers to meet project schedules while satisfying regulatory requirements and ambitious functional requirements was uncertain.

- Finally, the IPSN regulators had serious reservations about the capability to perform proper V&V analyses on software generated by the CONTROCAD design tool because of its complexity.

The schedule interruption and technical concerns caused EdF to abandon the P20 system and select an entirely new vendor for the control and monitoring system of Chooz B. Following the decision by EdF, British Energy also abandoned the P20 system for Sizewell B.

It can be concluded that one of the primary technical difficulties faced by the P20 system was that the software for the system had become too complex to be verified effectively and confidently. This resulted from a combination of the complexity of an unproven computing platform and the difficulty in evaluating the quality of the software product from the code design tool. One outcome of this experience is the development by EdF of guidelines for the use of software tools.

Canada

In preparation for the first Darlington operating license, the Canadian Nuclear Safety Commission (CNSC) indicated that before the redesign of the shutdown system software started, a suitable standard must be developed. Afterward, Ontario Power Generation, Inc. (OPG) and Atomic Energy of Canada, Ltd. (AECL), developed the Standard for Software Engineering of Safety Critical Software (OPG/AECL Standard, CE1001 Std Rev.1-1995 "Standard for Software Engineering of Safety Critical Software", referred to as CE-1001). CNSC staff monitored the development of this standard. OPG and AECL started from IEC 60880-1986 "Software for computers in safety systems of nuclear power stations" and a survey of other international standards, and incorporated the advice of renowned software experts. CNSC found that the CE-1001 satisfactorily addressed the concerns it had with the development of the original shutdown system software. CE-1001 emphasizes formal software review and maintainability, including formal requirements and specifications.

Following development of CE-1001, OPG and AECL produced a series of procedures, work practices, tools, and guidelines contained in the Standards and Procedures Handbook (OPG Document, 1998) for the redesign of the Darlington Shut Down System #1 (SDS1) and Shut Down System #2 (SDS2) software. The CNSC staff reviewed the standards and procedures related to software development and determined that they would ensure the production of reviewable and maintainable software.

The Darlington plant trip computer software was developed using the spiral model. In this approach, each phase chosen around the spiral loop yields a comprehensive product without incurring the full design documentation overhead. The CNSC staff found the use of the spiral model acceptable. Because the software requirements were not stable before development began, several functional changes were anticipated. Eventually, only two loops around the spiral were necessary to complete the design.

Two different specification formats, one for SDS1 and another for SDS2, were used to achieve diversity for software production. For SDS1, the trip computer design requirements and design description consisted of an English overview description and a corresponding mathematical functional description based on a box-structured method. The design description described the

interface requirements between hardware and software components. The required software functions contained in the design requirements and design were combined to form the "virtual" trip computer software requirement specifications.

For SDS2, the software requirement specifications were written using function tables. The CNSC staff found the specifications to be complete and correct with respect to the system requirements. They also determined that the specifications would lead to software that was easy to modify and test. The licensee chose a development approach that met the regulatory requirement of design diversity between the two shutdown systems.

Systematic design verification involved providing objective evidence that the behavior of every output in the software design met the software requirement specifications. The verification approach adopted provided evidence that the software design performed all functions specified and did not perform any unintended functions. The CNSC staff insisted that the group of verifiers must be independent of the group responsible for design and implementation of the software.

For both SDS1 and SDS2, the licensee performed unit testing, software integration testing, validation testing, system integration testing, and reliability qualification. The CNSC staff followed and reviewed the testing activities and found that minor deviations from the system specification occurred during the first loop of the software cycle. Those deviations were effectively dealt with using a discrepancy and change resolution process.

Reliability qualification is a testing technique, based on statistical observations, which is used to estimate the probability of software failing to meet its functional requirements. Given the developmental nature of this field (i.e., statistical testing), the CNSC staff did not have a high degree of confidence in the numerical results of reliability qualification. However, it was a useful and diverse validation of software behavior. Eight thousand test cases were run for each shutdown system software. Fewer than 5 percent of the results were found to be discrepant, and those discrepancies were caused by limitations of the testing rig, rather than software faults.

Commissioning activities performed by the licensee included a subset of tests to provide additional confidence that the trip, display/test, and monitor computer software met their specified functional requirements. OPG prepared an SDS1/SDS2 installation guide, and SDS1/SDS2 commissioning specification, which were consistent with the plant operating procedures. CNSC staff was involved in reviewing the guidelines and approving the documents associated with temporary and permanent changes. The installation of the redesigned shutdown system trip computer software on all four units was completed in late 1999.

Switzerland

The principal issue surrounding the HSK regulatory approval of the ANIS for the Beznau Nuclear Power Station concerned the possibility that the logic in the database(s) of the computerized procedures and/or the alarm system might be flawed in a way that would mislead the control room operating staff to perform an incorrect action. This concern was initiated by the French regulatory authority (IPSN). During the regulatory review of the N4 control room, IPSN discovered that the computerized presentation of the operating procedures performed a

comparison of the demands of the current procedure step against the current plant state. The French regulatory authority insisted that the procedure steps be presented separately from the current plant conditions so that any conclusions regarding actions to be taken must be made by operators and not the computer.

The ANIS computerized procedure presentation system performs this comparison and advises the control room staff of the satisfaction/completeness of each procedure step. By doing so, the Beznau control room operators can address malfunctions much more quickly, thereby reducing the time the plant process is beyond design limits, thereby potentially limiting the severity of transients. This benefit was so important to the Beznau Operations Department that they devised an entirely new "method of operation" for plant operation and procedure use.

The concern of the French regulatory authority caused roughly a 3-year delay in getting the ANIS approved by the Swiss regulatory authority. It was during this period that the Swiss regulatory authority required Beznau to conduct an independent third-party review of the significant portions of the computerized procedure database and the alarm logic database. Beznau was also required to perform extensive additional simulator demonstrations and formal tests in the presence of members from both the French and Swiss regulatory authorities.

3.6 Software Errors

United Kingdom

Commissioning testing of HICS at the Sizewell B Nuclear Power Station revealed an error in the system software. The software error, which was in the data network controller, was easy to uncover and reproduce. Under burdened operation, the data buffer management could corrupt the data. The problem occurred at a threshold, so it was easily detected after the threshold was reached. However, the software error was a subtle problem with dynamic data buffers that is not amenable to analysis using formal methods. Nevertheless, the problem was localized and readily corrected.

A root-cause analysis was undertaken immediately. The same software module is part of the Sizewell B PPS software. Moreover, the PPS software had completed both the Westinghouse and British Energy verification programs. The PPS uses the same data network design, but the number of nodes is small. The analysis showed that, in the limited PPS application, the threshold was not reached and a malfunction of the software would not occur. Therefore, the defect was not classified as a PPS software error. It was agreed that a normal PPS software maintenance update could include the HICS software correction, but the PPS software would not be updated solely to include that correction.

Sweden

The AC160 supplied by ABB was selected for application to the reactor protection system of the Oskarshamn Nuclear Power Station Unit 1. The ABB AC160 had been previously certified for boiler protection in Germany by the TÜV Nord regulatory authority, which has regulatory purview beyond nuclear applications. To satisfy Swedish regulations, the AC160 software design and verification process was amended to meet the requirements of IEC-60880. The

software implementation by ABB, however, did not strictly meet the recommendations of IEC-60880. For example, the use of interruptible structures and multitasking did not follow IEC-60880 recommendations. During this process, errors in the AC160 controller software and software tools were discovered. To address these defects, ABB performed an extensive "add quality" process on the AC160 software. In effect, the "add quality" process reworked the AC160 software design and verification process so that it met the requirements of IEC-60880 and addressed the reported software errors. To reduce the complexity of this process, ABB removed features from the nuclear product line of the AC160 controller software and software tools.

Korea

In 1999, an incident at Uljin Nuclear Power Station Unit 3 corrupted data on the performance net of the DPCS. This incident was caused by a failure of the application-specific integrated circuit (ASIC) chip on the rehostable module, which is part of the network interface module. The data communication architecture of the DPCS has a dual-ring topology. The incident occurred at the end of the first cycle over an interval of approximately 8 hours. The plant was in normal operation, but several non-safety components displayed abnormal behaviors. For example, several pumps that were not in operation suddenly started without any demand, some closed valves opened and other open valves closed, and some circuit breakers used in tying electrical buses switched on or off. Intermittent chattering of relays also occurred. Due to the response of the operators and diverse systems, the incident was mitigated without adverse consequences. A review of the system found that a common-cause software error was the likely cause. It was found that there was no provision to protect against foreign writes in the global memories within the communication network. As a result, software modifications were implemented that included a change of data format, mirror testing, status testing, and hardware foreign write protection.

The safety-critical interlock signals were hardwired at the request of KINS. The safety-related components operated normally despite the communication failure. As a result, a hardwired backup panel was installed to prevent software common-mode failures. However, reviewers concluded that the system architecture was still vulnerable to a foreign write in the rehostable module despite the presence of foreign write protection. Therefore, all safety-related signals were hardwired to make up for the vulnerability of the system architecture. As an added measure, KINS required the installation of an alarm window in the MCR to alert operators of possible network failures and development of an abnormal operations procedure to address possible control system failures caused by data communication errors.

3.7 Hardware Failures

Japan

In 2001, a failure of control rod transponder circuit boards at Kashiwazaki-Kariwa Nuclear Power Station Unit 5 rendered the control rods inoperable. Following detection of the defective cards, an analysis revealed that the failure mechanism was aluminum (Al) wire breakage in the integrated circuits (ICs) caused by electromigration. The particular ICs used at Kashiwazaki-Kariwa were manufactured at Hitachi Takaski Works. It was discovered that, from 1985 to

1990, ICs manufactured at that plant that contained Al crystal grain sizes that were too small, which contributed to their susceptibility to electromigration. The utility, Tokyo Electric Power Company, replaced all of the affected boards, and the manufacturer confirmed that quality control methods for the IC manufacturing process subsequently improved.

Electromigration is the transport of metal atoms induced by high electric current. The effect of electromigration is typically negligible for discrete and medium-scale IC components. However, at the level of miniaturization of current very large-scale integrated (VLSI) circuits, the current density of metal interconnects and/or inter-level contacts is high enough ($\sim 10^6$ A/cm^2) to increase the likelihood of occurrence of this phenomenon. The mechanism for this phenomenon is high-current loading, which causes an increase in interconnect temperature due to Joule heating. This Joule heating results in the creation of voids that lead to the failure of the metal interconnects. The mass flow of the metal atoms takes place in the form of diffusion along interfaces (such as grain boundaries and surfaces) and volume diffusion. In Al interconnects, grain boundary and interface diffusion are the dominating transport mechanisms at operating conditions (temperatures below 250°C). Thus, the small grain sizes of the ICs at Kashiwazaki-Kariwa provided ample interfaces to promote the metal migration.

As stated, Hitachi and its IC suppliers improved their quality control. In particular, the IC suppliers have improved their processes since the late 1980s by developing standard sample, accelerated test methods applied at the IC development stage. Through these evaluations, IC suppliers establish reliability targets and control IC quality. Concurrently, the Hitachi Information and Control Systems Division has improved its analysis methods for failed ICs that occur in the field and promoted more effective use of field data in accrediting IC suppliers. Presently, Hitachi follows a multistage quality control process for its digital products. The process begins with an accreditation process involving evaluation of the quality controls and product performance of the IC supplier. As part of this process, a series of IC qualification tests are conducted (see Table 3.1). Hitachi now performs IC acceptance tests after purchase of ICs from an accredited supplier (see Table 3.2). Following component assembly, Hitachi also performs printed circuit board tests (see Table 3.3). Any failure detected during testing or field use prompts a failure investigation and analysis (see Table 3.4), with the results leading to improvement requests directed to the IC supplier.

Table 3.1 IC Qualification Tests (Accreditation)

Qualification Test Item	Content	Test Equipment
Preliminary evaluation	Document and reliability data	---
Appearance & dimension	---	Stereomicroscope
Workability	Heat-resistance to solder, chemical-proof, etc.	Solder bath
Characteristic test	Electrical and function test	VLSI tester
Heat test	Characteristic test at low, normal and high temperature	Variable temperature control box
X-ray vision	Inner workings	X-ray fluoroscope, ultrasonic image scanner
Withstand voltage test	---	Curve tracer
Electrostatic resistance	Electrostatic discharge voltage	Electrostatic discharge tester
Thermal shock test	Thermal stress strength	Thermal shock tester
Operation life test at high temperature*	(acceleration life test)	Burn-in tester
Life test at high temperature & high humidity*	(acceleration life test)	Variable temperature and humidity control box, Unsaturated heat-cooker
Disassemble	Evaluation of inner workings and materials	Metaloscope, Scanning microscope

* These tests are implemented by IC suppliers. Hitachi reviews the data.

Table 3.2 IC Acceptance Tests

Test Item		Remarks
Appearance		
Thermal shock test		
Characteristic test		
Lot-by-lot sampling tests:	X-ray vision	Short-term test (first stage test)
	Disassemble	
	Life test at high humidity (heat-cooker)	
	Characteristic test	
	Burn-in test	Long-term test (second stage test)
	Characteristic test	

Table 3.3 Printed Circuit Board Tests

Test Item	Content	Test Equipment
Component assembly check	Checking a correct components' mounting and solder treatment	Component assembly checker (image scanner), 3D X-ray tester
Open / short circuit check	Checking a print-circuit mis-bonding	In-circuit tester
Dielectric measurement	---	Automatic dielectric with stand tester
Aging test	Exposing to high-temperature environment for specified time	Variable temperature and humidity control box
Operation test	Accuracy, function, response time, etc.	---
Power source	Stable operation at low voltage and high voltage	Variable voltage regulator
Thermal test	Stable operation at low temperature and high temperature	Variable temperature control box

Note; Table 3 shows the typical test items of a printed circuit-board.

Table 3.4 Failure Investigation and Analysis

Test Item	Content	Test Equipment
Voltage-current characteristics measurement	---	Curve tracer
Input-output characteristics measurement	---	In-circuit tester
X-ray and ultrasonic vision	Checking inner workings and wiring such as open circuit	X-ray fluoroscope, ultrasonic image scanner
Microscopic observation of failed IC	---	Scanning electron microscope

4. REGULATORY PROCESSES AND ISSUES

A survey of international regulatory processes that were employed in licensing digital I&C systems at evolutionary nuclear power plants was conducted during this study. The findings established the context in which the advanced I&C technologies were reviewed and licensed. In addition, these findings contributed to an understanding of how similarities and differences in regulatory requirements and review approaches can facilitate or inhibit an effective licensing process for advanced I&C technology.

In this section, an overview of regulatory regimes from the international community is provided. Next, selected regulatory approaches applicable to advanced I&C technology are discussed. Finally, key regulatory issues are identified that were addressed in particular digital I&C licensing examples from this survey. Additional information on the regulatory regime and licensing experience for several countries can be found in a report entitled "Four-Party Regulatory Consensus Report on the Safety Case for Computer-Based Systems in Nuclear Power Plants," which the NRC prepared issued in 1997, and a report entitled "Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants," which the International Atomic Energy Agency (IAEA) published in 2002.

4.1 International Regulatory Regimes

United Kingdom

The Nuclear Installations Act of 1965 is the primary statutory basis for licensing nuclear power plants in the United Kingdom. Under this act, no site may be used for the construction or operation of any commercial nuclear installation unless the Health and Safety Executive (HSE) has granted a nuclear site license. The HSE has delegated responsibility for administration of this licensing function to the Nuclear Safety Directorate (NSD), which encompasses the Nuclear Installations Inspectorate (NII).

The goal of the NSD is to ensure proper control of risks to peoples' health and safety resulting from work activities on licensed nuclear sites. The NESD comprises three divisions, including inspection, assessment, and strategy/resource management. The inspection division is primarily responsible for carrying out site inspection activities to confirm that licensees are complying with their legal obligations. The assessment division develops standards and provides specialist technical advice on the adequacy of the licensees' safety cases. The strategy/resource management division develops strategies that enable the NSD to meet its objectives and undertakes project management activities for the directorate.

The NSD establishes general safety requirements to address the risks at a nuclear site. In addition, the directorate provides guidance in the form of safety principles. Licensees demonstrate their compliance with these requirements and principles by generating and maintaining a "safety case" and procedures to satisfy license conditions. The "safety case" provides the documentation of the safety analysis developed to demonstrate how the plant will operate within the guidance and safety requirements.

France

The responsibility of nuclear safety in France is placed on the nuclear operator. The provisions taken by the nuclear operator to ensure nuclear safety are supervised by the Nuclear Safety Authority (*Autorité de Sûreté Nucléaire*), which acts under the joint authority of the Ministry of Environment, the Ministry of Industry, and the Ministry of Health. The central organization within this independent authority is the General Directorate for Nuclear Safety and Radioprotection (DGSNR or *Direction Générale de la Sûreté Nucléaire et de la Radioprotection*). The primary responsibilities of the DGSNR include developing general technical regulations concerning the safety of nuclear installations, licensing nuclear installations, and inspecting and monitoring nuclear installations. The DGSNR draws on the expertise of the Institute of Radiological Protection and Nuclear Safety (IRSN or *Institut de Radioprotection et de Sûreté Nucléaire*). The IRSN is composed of the Institute for Nuclear Protection and Safety (IPSN or *Institut de Protection et de Sûreté Nucléaire*) and the Office for Protection against Ionizing Rays (OPRI or *Office de Protection Contre les Rayonnements Ionisants*). At the request of DGSNR, the IRSN performs safety analyses to evaluate provisions proposed by the nuclear plant operators. For matters such as major modifications to nuclear installations or examination of preliminary, intermediate, and final safety analysis reports, the DGSNR requests the opinion of expert advisory committees (*Groupe Permanents d'Experts*). For other matters, such as minor modification to plants or provisions made to address minor incidents, the safety analyses conducted by IRSN give rise to recommendations that are transmitted directly to the DGSNR.

Canada

The Canadian nuclear industry consists of a mixture of public organizations and private firms. At the federal level, the CNSC is empowered to make all regulations governing all aspects of the development and application of nuclear energy. The CNSC reports to the Canadian Parliament through the Minister of Natural Resources. The Canadian licensing process requires the licensee to prove that the nuclear plant operations are safe. The safety of operating nuclear power plants is reviewed for compliance with the requirements of CNSC, industry codes and standards, and pertinent policies and procedures.

Japan

Regulatory authority for nuclear reactors in Japan is established in the Electric Utility Industry Law and the Law for the Regulation of Nuclear Source Material, Nuclear Fuel Material, and Nuclear Reactors. The Ministry of Economy, Trade, and Industry (METI) has responsibility for approving the construction and operation of commercial nuclear power plants. Within METI, the Agency of Natural Resources and Energy (ANRE) addresses nuclear power issues and actions. The Nuclear and Industrial Safety Agency (NISA), which reports to ANRE, has the central role in safety regulation of commercial nuclear power. Its responsibilities include generation of safety regulations, licensing of facilities and processes engaged in all aspects of the nuclear fuel cycle, and oversight of commercial nuclear plants. The Ministry of Education, Culture, Sports, Science, and Technology (MEXT) and the Nuclear Safety Commission (NSC) of the Atomic Energy Commission also have advice and consent roles in the approval process for reactor installations. The licensing process involves authorization for a nuclear power installation followed by permission for the construction and operation of the power plant. During

this approval process, Japan employs a double check system of nuclear safety review employing NISA and NSC.

The Japanese safety regulation system is largely based on a voluntary assurance system administered by the electric utility industry. Thus, the main governmental regulatory role is largely one of approval, and the utilities are responsible for ensuring nuclear safety. However, the Japanese government is very active in sponsoring collaborative research supporting nuclear safety. In particular, the Nuclear Power Engineering Test Center (NUPEC) performs safety research to establish data and methods that provide the necessary basis for standards and guidelines.

Korea

The Ministry of Science and Technology (MOST) has responsibility for protecting public health and safety through regulatory control and safety inspections of nuclear installations. KINS performs technical assessment of licensee submittals and conducts safety inspections for MOST. However, the ultimate responsibility for nuclear safety rests with the operating organizations for nuclear plants in Korea. The licensing of nuclear power plants in Korea consists of a three-stage process, including site selection, construction, and operation. In addition, the Nuclear Safety Commission (NSC), an independent body that advises MOST, performs periodic safety reviews.

Czech Republic

The national regulatory authority in nuclear safety and radiation protection for the Czech Republic is the State Office for Nuclear Safety (SÚJB or *Státni Úřad pro Jadernou Bezpečnost*). The Atomic Act on the Peaceful Utilization of Nuclear Energy and Ionizing Radiation provides the legal framework for SÚJB. The Chairman of SÚJB acts as the Nuclear Safety Inspector General, with authority to appoint nuclear safety and radiation inspectors.

Sweden

The operators of nuclear facilities in Sweden have full responsibility for enacting the necessary steps to ensure safety. The Swedish Nuclear Power Inspectorate (SKI or *Statens kärnkraftinspektion*) within the Ministry of Environment is responsible for establishing a clear definition of safety requirements and monitoring compliance with those requirements. SKI ensures that Swedish nuclear installations have adequate defense-in-depth methods to prevent serious incidents or accidents originating from technical or organizational conditions; protects installations and nuclear materials against terrorism, sabotage, or theft; and provides for the final disposal of spent nuclear fuel and nuclear waste.

Switzerland

In Switzerland, a general license for the construction and operation of nuclear facilities much be granted before a technical license is issued. The Swiss Federal Council has responsibility for granting these licenses following consultation with the affected Cantons (provinces) and federal departments, and upon approval of the Federal Assembly (for general licenses). The Swiss Federal Nuclear Safety Inspectorate (HSK or *Haupabteilung für die Sicherheit der Kernanlagen*)

is responsible for reviewing the technical evidence submitted in support of license applications for nuclear facilities. Each license application must be accompanied by a technical report that demonstrates the safe operation of the facility under normal, abnormal, and accident conditions. Following review by technical experts, HSK provides a safety assessment report that includes conditions and recommendations. This assessment is submitted to the Federal Office of Energy, which solicits third-party input before the decision on issuance of the license by the Federal Council. Construction and operating licenses may be subdivided, with the construction license consisting of up to three sub-licenses and the operating license consisting of commissioning and operating elements.

4.2 International Regulatory Approaches

4.2.1 United Kingdom

4.2.1.1 Safety Philosophy

The safety philosophy in the United Kingdom adopts the "as low as reasonably practicable" (ALARP) approach to require that risk to the public must be maintained in the "tolerable" level. This "tolerability of risk" is defined in terms of three levels of risk:

- An "intolerable risk" is a risk that is so great or has an outcome that is so unacceptable that it must be rejected outright. The "intolerable risk" cannot be justified except in extraordinary circumstances.
- A minimal risk is one that is so small that no further precaution is necessary. A risk in this level is acceptable and requires no detailed work to show that risks are as low as reasonably practicable.
- A risk falling between these two states is one that has been reduced to the lowest level practicable, taking into account the benefits that will accrue from its acceptance and the cost of further risk reduction.

4.2.1.2 Licensing Procedures

It is the responsibility of the operating company to ensure the safety of a nuclear installation. Such companies must execute all license requirements to the satisfaction of the regulator. The NSD assesses the capability of the prospective operator to satisfy the safety requirements from design to decommissioning. NSD attaches license conditions to the site license and monitors the performance of the nuclear installation in adhering to those conditions. The current typical site license has 35 attached conditions covering such topics as safety cases, operating limits, training, and maintenance. NSD uses several controls derived from the license conditions, including giving consents, approvals, or directions. The arrangements may also require the licensee to obtain NSD's formal agreement before passing defined hold points.

All activities that affect safety in the nuclear industry are expected to be supported with a safety case. A safety case is the documented information and arguments that justify the safety of the plant, activity, operation, or modification under consideration. A safety case must be maintained throughout the plant's life cycle, and it may address the design, construction, and

commissioning of a new plant, modifications to existing plants, and the decommissioning of a plant.

Safety cases are intended to demonstrate how the proposed action (e.g., construction, modification, etc.) complies with the ALARP criteria and the licensee's health and safety standards. The safety case should be based on robust design; defense in depth; and deterministic analysis of normal operations, design-basis accidents, and severe accidents. In addition, the deterministic analysis should be supplemented by a probabilistic safety analysis to reveal any potential design weaknesses and confirm that reliability goals are met.

The safety case is the end product of a licensee's assessment of a proposed activity. NSD assesses a safety case to establish confidence in the arguments advanced by the licensee and to determine if the latter has, as a minimum, met its own criteria and demonstrated that the risks are ALARP. The licensee is responsible for safety at all times, and NSD requires that the licensee undertakes adequate peer review and independent assessment of its safety cases.

4.2.1.3 Guidance

To have a uniform approach for assessing licensees' safety cases, the NSD has published sets of criteria against which safety cases are judged. These criteria are called Safety Assessment Principles (SAPs). Not all of these principles are applicable to every plant. However, the extent to which the applicable principles are met has a direct bearing on decisions to grant or deny a license change. The SAPs contain guidance on good engineering principles that may be regarded as the basis for safe design, and overall risk targets that are derived from the tolerability of risk criteria. Other SAPs relate to diversity of fault detection, adequacy of margins, appropriate interfaces to plant operators or alarm systems, independence of function and independence of failure, reliability, testing, and maintenance of the safety system.

Where system reliability is significantly dependent on computer software, the appropriate SAPs promote demonstration that (1) accepted standards have been thoroughly applied, (2) adequate quality assurance has been implemented, (3) complete and preferably diverse checks are carried out on the final software by an independent team, and (4) a comprehensive and independently assessed test program is applied to check every system function and demonstrate system reliability. For these software-based safety systems, the assessment addresses the software development process based on criteria derived from an accepted model for the software development life cycle. While the criteria are not a set of mandatory conditions, they provide guidance for assessors when examining software designs and their associated safety cases.

4.2.2 France

4.2.2.1 Safety Philosophy

French nuclear safety philosophy is based on the principle of defense-in-depth. This principle requires the provision of a series of safety layers, with each layer aimed at offsetting design-basis events and accidents. Each safety layer is required to be as reliable as possible, but the extremely low accident probabilities associated with nuclear safety requirements can only be achieved when the impact of the various safety layers is assessed collectively. The French

defense-in-depth approach also postulates the failure of all preventive measures taken and the occurrence of accident scenarios, the consequences of which must then be mitigated.

Overall, the French nuclear safety approach is deterministic. However, this deterministic approach is also supplemented by probabilistic assessments to estimate the safety level achieved and to identify weak points in the installation.

4.2.2.2 Licensing Procedures

In France, regulation of basic nuclear installations (BNIs), which includes nuclear power plants, involves an authorization decree procedure followed by a series of licenses issued at key points in during the life of a plant, including fuel loading or precommissioning tests, startup of normal operation, decommissioning, and dismantling.

The application of these various procedures starts with site selection and plant design and ends with the ultimate site dismantling, as follows:

- An operator who decides to build a new type of BNI is expected to present the relevant safety objectives and the main characteristics as early as possible, and well before submitting the authorization application.
- Based on an analysis by the IRSN, the DGSNR asks the competent advisory committee to formally examine the proposals submitted.
- The DGSNR informs the operator of the issues that must be covered by its authorization decree application.
- Application for the BNI authorization decree (plant authorization decree) is sent to the Minister for the Environment and the Minister for Industry, who forward it to other ministers concerned, such as the interior and health ministries. As a minimum, the application file includes a description of the main characteristics of the planned installation, location drawings, and a preliminary safety analysis report.
- The processing of the operator's application includes a public inquiry and a technical assessment. Note that the preparatory application procedures identified in the first three bullets do not exempt the applicant from this technical assessment or any other regulatory examination; rather, they simply facilitate the application processing procedure.
- Six months before fuel loading, the operator must submit a provisional report with provisional general operating rules and an internal emergency plan. The DGSNR consults the Advisory Committee for Reactors on these documents before drafting its own recommendations. The ministers can authorize fuel loading and precommissioning tests upon receiving the recommendations from DGSNR.
- The first core load can only be delivered to the new fuel storage after authorization by the Ministers for the Environment and for Industry. This authorization is granted only after the DGSNR has (1) examined the storage facility provided by the operator (presented at least 3 months beforehand), and (2) reviewed the conclusions of an inspection carried out just before the date fixed for the delivery of the fuel elements.
- Four successive licenses are required in the startup stages for a PWR. Specifically, these include a fuel loading license, a license for precritical hot testing, a license for first

criticality and power escalation to 90 percent of nominal, and a license for power up to 100 percent of nominal.

- After the initial startup, the operator requests the issuance of a definitive commissioning license. The request must be made within a time limit stipulated in the authorization basis. The operator's request is substantiated by a final safety analysis report, final general operating rules ,and a revised version of the internal emergency plan. These documents must reflect the experience acquired during the operating period since initial startup.

4.2.2.3 Guidance

Technical nuclear safety rules are provided in a set of regulatory texts ranging from very general to specific and detailed, as follows:

- General technical regulations

  The general technical regulations deal with the two main areas of quality and pressure vessels. Two ministerial orders specific to BNIs address these areas.

- Basic Safety Rules

  The DGSNR issues basic safety rules (RFSs) on various technical subjects. There are about 40 RFSs in all. These basic safety rules provide recommendations defining the safety objectives to be achieved in different technical fields and describe accepted practices with these objectives. Although they may be seen as the equivalent of the NRC's regulatory guides, they are not, strictly speaking, regulatory documents. In particular, a plant operator is not obligated to adhere to the RFSs, provided that the operator can demonstrate that the safety objectives underlying the rule can be achieved by alternative means. Thus the RFSs provide great flexibility, allowing for technical advances and new technical knowledge.

- Design and Construction Rules

  Regulations require the operator to submit a document defining the rules, codes, and standards that will be used for the design, construction, and startup of safety-related equipment. The main codes and standards are known as the Design and Construction Rules (RCCs). Many of these rules are published by the French Association for Design and Construction Rules for Nuclear Steam Supply System Equipment. Framatome and EdF are members of this association. Although DGSNR is not responsible for drawing up the documents, it examines them in detail, both in their initial and final versions.

4.2.3 Canada

4.2.3.1 Safety Philosophy

The safety approach used in Canada is to ensure that the risk to the public presented by nuclear power plants is substantially lower than that from alternative sources of energy. This approach includes numerical safety goals to ensure that the likelihood of a serious release of fission products is negligibly small. A fundamental principle of the regulatory approach is that

the licensee bears the basic responsibility for plant safety. The basic consideration applied is that no technology is fail proof, so licensees must incorporate multiple layers of protection.

4.2.3.2 Licensing Procedures

CNSR regulations with respect nuclear power plants are primarily procedural. The board sets the general requirements for reactor design and operation, and then leaves it to the licensee to develop the processes necessary to meet those requirements. In this sense, designers have a considerable degree of freedom to design nuclear plants to meet the regulatory criteria. Over the years, this approach has led to the gradual establishment of acceptable safety features for CANDU power plants. CNSR holds further discussions with the applicant if a new design does not contain these design features.

Software for safety-related systems should be submitted for assessment by the CNSR at the following specific points during the development of the software:

- At the beginning of the software development project, a licensee should submit an analysis of the system criticality and categorization of the software, plus the appropriate standards, plans, and procedures.
- When the system and software requirement specifications have been completed, a licensee should submit the requirements, including corresponding test plans. System requirements and testing are discussed in further detail in the next section.
- Near the end of the project, a licensee should submit the results of the systematic inspection of the software, including how the analysis of the system hazards has been addressed. Systematic inspection requirements are discussed in the next section.
- At the close of the project, a licensee should submit software and system test reports. Testing requirements are discussed in the next section.

4.2.3.3 Guidance

The basic requirements set limits on both the frequency of serious process failures and the availability of safety systems. CNSR defines a "serious process failure" as any failure of process equipment or procedure that, without special safety system action, could lead to significant release of radioactive material from the station. The special safety systems include the reactor shutdown system, the emergency core cooling systems, and the containment system.

Basic Guidance on Software

When control and protection are provided by computer software, licensees are required to submit sufficient evidence that the software is complete, correct, and safe. The documentation provided to demonstrate these characteristics has to be independently reviewed. Licensees categorize the software at various levels according to criticality or the impact of possible software failures. The degree of formality and completeness in software development, analysis, and verification is then made dependent on the criticality level to which the software is assigned.

Software categorized as the most critical to safety is called "safety-critical" software. Safety-critical software should meet the full range of criteria described below. Less critical software should still meet the same criteria, but to a less detailed level. Areas that may be relaxed for less critical software include (1) the degree of mathematical formality of specification and verification, (2) the extent of the hazard analysis (e.g., if the system level hazard analysis shows that a software failure cannot have a serious impact, then further hazard analysis may not be necessary), and (3) the amount of testing required.

Safety-critical software requirements should be unambiguous. Each requirement should be sufficiently precise that a test or verification is feasible to distinguish between correct and incorrect implementations. Software requirements should also be complete; in other words, they should cover any situation that could arise during operation. They should also define what the software must do, and should include functional, performance, safety, reliability, and maintenance requirements. The software requirements document should be sufficiently complete that if all requirements are demonstrably met, the software will be considered adequate and acceptable. Reliability requirements should specify the reliability targets for the software based on system- and component-level reliability targets.

System inspection of software design should include analysis of both the functionality and the safety of the software. Functional analysis should demonstrate that the software performs all required functions and does not perform any unintended functions. It should also verify that each product is complete, and should validate that the final system meets all system requirements and user needs.

Analysis of software safety should demonstrate that the software does not initiate any unsafe actions under expected operating and accident conditions. A system-level hazard analysis should identify system hazards and trace them through the system to determine the software contribution to each hazard. Safety-critical software must be sufficiently simple that a complete analysis of software safety is both feasible and credible. The software should also be isolated from non-critical software. Physical isolation by means of hardware is preferred to isolation using only software.

Analysis of software should include an analysis of both the expected and possible operations of the user interface. Software should be designed to incorporate fail-safe and fault-tolerant features where the increase in safety justifies the additional complexity. For example, in a situation in which a fail-safe feature increases the complexity of the software to the extent that safety analysis is doubtful, it becomes preferable to omit the software feature.

CNSR also provides guidance on software testing. The aim of software testing is to enable identification and removal of as many faults as reasonably possible (functional testing), and to establish confidence in the safety and reliability of the system (random testing). Software testing should include both functional and random testing. Functional testing exercises the software with inputs selected to cover the functionality and logic of the software. It should include integration testing and system testing, and may include unit testing if this is appropriate to the development method. Functional tests should also check the timing and performance requirements of the software running on the target computer.

Random testing should be statistically valid to establish confidence that a system will function without failure under specific operating conditions. Statistical validity should be demonstrated

by showing that many independent, randomly selected test cases have been run without failure. Input data selected for the random tests should accurately represent either real operating conditions, or operating conditions in the area of greatest concern. The number of tests should be related to the reliability requirements.

4.2.4 Korea

4.2.4.1 Safety Philosophy

Five regulatory principles drive the policies and procedures implemented by MOST. Specifically, those principles are independence, openness, clarity, efficiency, and reliability. Through application of those principles, MOST strives to secure consistency, adequacy, and rationality in its regulatory activities. Of primary importance in the Korean nuclear industry is adherence to the principle of "priority to safety." Since the operating organization bears responsibility for safety at commercial nuclear power plants in Korea, MOST encourages development of a safety culture and works to clearly define the necessary safety requirements that contribute to achieving and maintaining nuclear safety. Emphasis on diversity and defense-in-depth in its requirements are the primary means of establishing safety, and periodic safety reviews are intended to help maintain that condition.

4.2.4.2 Licensing Procedures

The regulation and licensing procedures are subdivided into three stages:

- In site selection, the conceptual design is examined to assess the appropriateness of the proposed site and the safety requirements of the site are reviewed in terms of design, construction, and operational issues.
- A construction permit application is contingent on review of the reference design, quality assurance program, preliminary safety analysis report (PSAR), and environmental impact statement.
- An operating license application is contingent on review of the operational technical specification and emergency plans and procedures. MOST also confirms that the as-built plant conforms to the reviewed design.

4.2.4.3 Guidance

The approach for classifying the safety importance of I&C systems is based on deterministic methods and engineering judgment, which focuses on the use of diverse I&C systems as a guard against software-related common-mode failures. The classification criterion is based on plant design bases such as design-basis events, special events including software common-mode failure, and normal operation. The diverse I&C systems are provided for special events such as ATWS and software common-mode failures of the reactor protection systems.

I&C systems are classified into four categories (i.e., IC-1, IC-2, IC-3 and Non-IC). The software for I&C systems is further classified into three categories, including safety-critical, safety-related, and non-safety-related. Safety-critical software must meet the most stringent standards and criteria. To address the potential for common-cause failures in safety-critical software, an independent diverse backup system is required. If the backup system is digital, its

software is classified as safety-related. Safety-related software is subject to less stringent practices and graded requirements than safety-critical software. The requirements of non-safety-related software may be tailored to account for its lower safety importance. The major differences among the three software categories relate to the extent and severity of V&V activities, software safety hazard analysis, configuration management activities, and quality assurance activities.

In summary, the IC-1 systems (e.g., reactor protection systems) must meet all of the safety requirements, but the IC-2 systems do not require analysis of defense-in-depth and diversity. The IC-3 systems are diverse I&C systems, which should be subject to environmental qualification and should be specially classified as safety-related software. Table 4.1 identifies some key requirements for each category.

Table 4.1 Key Requirements for I&C Systems According to Safety Category

Requirements	I&C Systems Important to Safety			I&C Systems Not Important to Safety
	Reactor Protection Systems (IC-1)	Safety-Related I&C Systems (IC-2)	Diverse I&C Systems (IC-3)	Non-Safety-Related I&C Systems (Non-IC)
Quality Assurance	Atomic Act -QA Req.s (similar as 10CFR50, App. B)	Atomic Act - QA Reqs. (similar as 10CFR50, App. B)	US NRC GL85-06	Plant QA Programs for Non-Safety Items
Single Failure Criteria	Required	Required or Not Required	Not Required	Not Required
Environmental Qualification	Required	Required	Required(*)	Required(*)
Seismic Qualification	Required	Required	Not Required	Not Required
Class 1E Criteria	Required	Required	Not Required	Not Required
D-I-D and Diversity Criteria	Required	Not Required	Not Required	Not Required
Software Category	Safety-Critical Software	Safety-Related Software	Safety-Related Software	Non-Safety-Related Software

* The environmental qualification should be done commensurate with the importance of the safety functions to be performed.

4.3 Regulatory Issues

4.3.1 Diversity and Defense in Depth

Recently, the regulatory concern about common-cause failure has focused on the use of computer software in reactor protection systems. Most regulatory authorities accept that for conventional systems, or the hardware of a computer-based system, comprehensive physical and electrical separation of the redundant equipment and the equipment services normally provides sufficient demonstration of defense against common-cause failures. In some cases, this may be an assumption of convenience, so a protection design comprising two separate systems can resolve the signal priority for the control of a single device. However, where a safety function is implemented by a software-based system, most regulatory authorities require at least one additional, demonstrably diverse and independent means of implementing that safety function.

Software-based digital systems are more complex than systems based on conventional analog technology. Nevertheless, operational experience shows that, when properly engineered, software-based digital systems are also more reliable than their analog counterparts. This added reliability largely derives from the fact that the calibration adjustments required for conventional analog systems are tedious and need to be done at regulator intervals because of instrument and equipment drift. Conventional designs also require relatively massive cabling both within the equipment cubicles and throughout the plant. By contrast, the proper operation of a microcomputer-based system can be more transparent than a conventional analog system because of the following factors:

- Internal variables are shown in engineering units.
- Multiplexed outputs accommodate viewing process and system internal variables without adding complexity to the design, disturbing the operation of the system, or requiring access to the protection system electronics cubicles.
- The operation of a software-based computer system is inherently dynamic, so system functioning can be readily discerned.
- The inclusion of cyclic hardware diagnostics within the software design can ensure proper operation of the hardware and can quickly identify hardware failures, thereby precluding latent failures in the system.
- The manual, routine operational testing for the conventional analog reactor protection systems requires reconfiguration of the protection circuits and takes considerable time to perform.

System classification is a significant requirement surrounding the diverse and independent means for actuating the safety system. For example, in the existing U.S. approach, the ATWS system is classified as a non-Class 1E system. Other regulatory authorities, such as the DGSNR in France, agree with this classification. However, some regulatory authorities, such as the NII in the U.K., require that a reactor protection system must comprise at least two Class 1E parts. The two different positions can be justified because of the subjective nature of the situation. On one hand, the functions being performed are safety functions, so they should be implemented with Class 1E designs. On the other hand, non-Class 1E design solutions are the most diverse and independent because the treatment can be very different and, therefore, less likely to share common flaws with a Class 1E design.

The complexity of the overall design solution should also be considered, and is especially important for emergency safety features functions. For example, the Temelin common-cause failure diversity requirements led to the need for a complete system, the Non-Programmable Logic (NPL), in addition to the two diverse systems. The NPL is not based on microprocessor technology. The NPL is needed to implement valve priority logic that prioritizes the commands from the diverse Class 1E systems and the non-Class 1E Reactor Limitations System, and it issues prioritized commands to the actuators. In addition, the NPL implements a part of the diesel load sequencing to address the potential for common-cause failures. This is an example where it is assumed that systems or logics that are based on conventional technology are not subject to common-cause failure.

The AP600 Diverse Actuation System (DAS) is an example where the design flexibility afforded by a non-Class 1E diverse system can lead to a significantly less complex solution. The

non-Class 1E DAS solution allows the DAS to interface to existing fluid systems, although generally at a different, non-safety point. Therefore, the AP600 design reduces the need for logic to prioritize signals from the reactor protection system and the DAS.

The case for protection system diversity and defense-in-depth must be made in conjunction with the nuclear plant safety case, taking into account all plant-specific factors. However, the Sizewell B nuclear power plant IPS itself has numerous features that will support the case. To monitor the operation of a Westinghouse PWR, many different types of sensors are used, especially when the evolutionary sensor types are employed. For example, postulated PWR events are covered by multiple measurements by different types of sensors. The manual reactor trip feature interfaces directly with the reactor trip breaker undervoltage coils and opens all eight circuit breakers. The reactor trip functions and engineered safety features functions are performed in completely independent microcomputer subsystems, including inputs and outputs, in order to separate independent functions that protect against the same event. The two-of-out-four logic facilitates plant arrangements with significant physical separation.

With failsafe design, if a common-mode failure occurs, it is still likely to lead to a safe state for the plant. The system software must be substantially constrained and subjected to an extensive V&V program. In addition, the system hardware design must be verified and tested to nuclear environmental and seismic qualification requirements.

The United States employs a structured qualitative methodology for analyzing diversity and defense-in-depth. This approach evaluates the vulnerability of the reactor protection system design with respect to common-cause failure. The methodology identifies several types of diversity that can be employed in the analysis:

- Human diversity is the effect of human beings on the design, development, installation, operation, and maintenance of systems.
- Design diversity involves the use of different approaches (including both software and hardware) to solve the same or similar problem.
- Software diversity involves the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals.
- Functional diversity involves the use of two systems that are functionally diverse because they perform different physical functions although they may have overlapping safety effects.
- Signal diversity is the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly.
- Equipment diversity is the use of different equipment to perform similar safety functions, where "different" means sufficiently unlike as to significantly decrease vulnerability to common-mode failure.

The regulatory authorities in other countries, such as France and Japan, impose requirements similar to 10 CFR Part 50.62, "Requirements for Reduction of Risk from Anticipated Transient without Scram (ATWS) Events for Light-Water Cooled Nuclear Power Plants," to addressg common-cause failures in microprocessor-based designs. Other countries have developed more prescriptive requirements.

The Czech Republic specifically requires that the reactor protection system must comprise two separate Class 1E parts. Each part must be capable of terminating and mitigating frequent design-basis events (i.e., those with a probability of occurrence greater than 1 in 1,000 per year) concurrent with a postulated common-cause software failure in either part, but not both simultaneously. This requirement resulted in a very complex software-based reactor protection system design.

The view in the UK in general, and in the regulatory agency in particular, is that as the level of claimed reliability increases, it becomes progressively more difficult to demonstrate freedom from common-cause failures. The judgment is that current methods of analysis, not necessarily the actual system reliability, limit the reliability that can be claimed for any single system. In particular, the UK regulatory position is that currently available methods are not capable of providing adequate demonstration below the level of 10^{-5} failures per demand. In addition, for novel or more complex designs, the practicable demonstration limit is considered to be higher (typically 10^{-4} failures per demand). Moreover, in order to meet even this level of reliability, the design must incorporate replication redundancy, as well as diversity, because of the potential for common-cause failures.

To support this requirement, four different systems perform Sizewell B Category 1 or Class 1E safety functions. The PPS and the SPS both perform the automatic safety functions. A major portion of HICS performs safety functions. Most of the HICS microcomputer system services software modules and hardware are of common design with the PPS, but are used to perform different control and supervisory functions. The load shedding and emergency load sequencing system is a conventional system that performs safety functions. Most of the safety case is based on, and most of the deliberation focuses on, the PPS and the SPS. The PPS has the diversity and defense-in-depth features described in the Westinghouse IPS discussion. However, these features were considered necessary just to meet the 10^{-4} failures per demand reliability criterion in the Sizewell B safety case.

At Temelin, a key design requirement imposed on the PRPS and the DPS is that the overall plant protection system can mitigate "frequent events" concurrent with a postulated common-mode failure in either the PRPS or DPS, but not both simultaneously. "Frequent events" are design-basis events with a probability of occurrence greater than 1 in 1,000 per year.

There are similarities and differences between the Sizewell B and Temelin protection system requirements related to common-cause failures. Both are based on frequent design-basis events. However, where the Sizewell B solution gives more emphasis to the PPS over the SPS based on numerical reliability, the Temelin requirements for the PRPS and the DPS are more symmetrical and place no numerical burden on either system.

The AP600 diversity and defense-in-depth analysis shows that the protection and safety monitoring system (PMS) is sufficiently reliable to meet the objectives of protection against all design-basis events and support meeting the plant's probabilistic safety assessment goals. A diverse I&C system, the DAS, is provided for unlikely common-mode failures of the PMS, for beyond-design-basis events, and to optimize the probabilistic safety assessment results. The fundamental goal is to protect against common-mode failure in the protection and safety monitoring system. The main common-mode failure issue is system microprocessor hardware and software failures. Common-mode failures of ventilation systems and power sources are

also considered credible. Seismic events are not considered to be initiators for common-mode failures.

For the SPIN platform, the case for protection system diversity and defense-in-depth must be made in conjunction with the nuclear plant safety case, taking into account all plant-specific factors. However, the SPIN itself has many features that support the protection system diversity and defense-in-depth case. The defense-in-depth implementation is not as distinct because, for a division or separation group, sensor signals are collected at a single, albeit redundant, point and then retransmitted to the control (prevention) function, reactor trip (termination) function, and safety features (mitigation) function. The defense-in-depth implementation is not as distinct because signals for reactor trip (termination) voting and safety features (mitigation) logic and voting are transmitted on the same network. Galvanic isolation is also not as robust as fiber optic isolation.

In France, the N4 reactor designs have a manual reactor trip that operates separately from the SPIN electronics and does not require electronics apart from the reactor trip breakers. The original design of the N4 control room had a small "safety panel," with perhaps a dozen discrete switches. These were system-level actuation switches for the Safety Class 1E emergency safety features systems. These switches interface with SPIN. EdF has since added a panel that contains discrete actuation switches for most of the individual safety system process components. These switches interface with the Contronic control system, which is not a Class 1E system.

4.3.2 Safety Classification Normally Associated with ATWS

Safety classification can provide a practical approach to allocate resources during design and licensing. The safety classifications used in today's nuclear power plants are defined in standards, but deviations exist in the various classification definitions.

The regulatory authorities in countries such as France and Japan impose requirements for addressing common cause failures in microprocessor-based designs that are similar to 10 CFR Part 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light Water Cooled Nuclear Power Plants." Other countries have developed more prescriptive requirements.

Although regulatory authorities and standards committees generally agree on the scope of Class 1E or Category 1 functions, some regulatory authorities place a different emphasis on certain areas. For example, the UK devotes more attention to automatic functions than to the manual control of individual safety features components. In addition, late in the design process for the Chooz B N4 plant, EdF added a panel that contains discrete actuation switches for most of the individual safety components. The switches on the panel interface with the Contronic control system, which is not a Class 1E system. In Korea, the hardware of the diverse backup shutdown system is considered non-safety-related, while the software is considered safety-related.

4.3.3 Commercial Off-the-Shelf Hardware and Software

The use of COTS systems dedicated for Class 1E application has received much attention in the United States, but not in other countries with large nuclear programs. In many countries, nuclear I&C system vendors remain the preferred suppliers for product lines that are specifically qualified for nuclear application. In Japan, because of tradition, ownership, quality assurance, and obsolescence considerations, the preferred approach is to design everything "from scratch." Nevertheless, there is an incentive (based on economics and availability) that prompts consideration of COTS hardware and software. In addition, the hardware components (such as microprocessors and circuit boards) have not generally been appropriately treated as COTS.

For COTS software, operational experience must not be the sole basis for establishing quality and reliability. This is because the licensee does not control the software development process. Thus, there are difficulties in establishing the relevance of experience for similar but not identical applications. Also, if the dedication process requires modifications to satisfy safety requirements, the difficulty in establishing a link with past operational experience increases.

Significant issues that may affect any COTS dedication approach are rapid obsolescence and configuration management. For example, commercially distributed digital control systems are rapidly changing at the present time. While the rapid advancement of technology is one factor, another is that these systems are past the point of mimicking conventional analog control systems and are expanding, in an integrated fashion, into the areas of data management and plant supervision. Thus, the foundational software packages are evolving with new features and functions being added to each revision. Updating non-safety system software to expand its capabilities may be desirable, but safety-related software must be maintained in a dedicated configuration in strict adherence to an imposed quality assurance program. Additionally, the accelerated pace of integrated circuit (IC) development limits the lifetime of a product line. Care must be taken to ensure that replacement parts use the same version of the same IC.

The application of the AC160 to Class 1E functions may be considered an example of dedication of commercial equipment. The controller is primarily used in fossil-fueled plant applications in general, and for boiler control and turbine control in particular. Predecessor designs (namely the AC700 and AC110) have seen widespread application in Europe. The dedication was facilitated by an "add quality" process in which features were removed from the nuclear version of the AC160 controller and tool software.

5. LESSONS LEARNED

5.1 I&C System Architectures

The communication networks have typically been the "weak link" in evolutionary plant architectures, with communications technology limiting the overall throughput of the architecture. The number of networks involved in any given architecture has been governed primarily by the available communications technology and the amount of data that must be put through the system to meet the system's functionality requirements. As a result, the most recent architectures employ the fewest number of networks as the technology has improved their capacity.

Often, the networks employed, particularly for the lower levels (e.g., data acquisition) of the architecture, are a vendor's proprietary design. The upper levels tend to use "open architecture" protocols, such as Ethernet (copper) or fiber distributed data interface (FDDI optical fiber). In most designs, requirements for "isolation" between those portions of the architecture that are designed to be Safety Class 1E and those that are not safety-related are met by fiber optic links rather than galvanic means.

The cost reductions have been dramatic relative to building physical volume, signal and control cable quantity and pulling, and support structures throughout the plant. When compared to solutions based on conventional analog technology, studies show that, if properly exploited, this feature can justify the cost of the entire system in a new plant application. Multiplexing also provides needed flexibility for backfit applications.

So far, microprocessor and workstation processing power has significantly outperformed communications throughput. Architecture design is fundamentally the process of collecting or arranging sets of computational platforms to perform traditional functions by sharing a common process-variable database. Little or no attempt has been made to break up and distribute the functionality in ways that would optimize the amount or productivity of the software and, in the process, probably improve the reliability of software and database maintenance. As a result, commonly used or calculated variables, such as steam table results, are found calculated in multiple locations throughout the typical architecture.

The commercial process control business has recently become very interested in being able to extract data and information from the plant I&C system to support plant "enterprise management." The desire to incorporate similar automation into the operation of nuclear power plants is a significant and growing factor in the decision process to upgrade the plant I&C systems.

In spite of the desire by some customers to use PC-based architectures and common industrial HSIs (such as Microsoft's Windows® technology), nuclear power plant I&C architectures have remained in the domain of the more robust UNIX-based servers, workstations, operating systems, and applications software. This is because designers, to date, have not been convinced that the data collection, processing, and communications demands of nuclear power plants can be adequately met, under all operating conditions, by the lower-cost, but less reliable Windows® technology, particularly during abnormal event (i.e., high data load and processing) conditions.

The regulatory view of the origin of possible operational errors and how to design to prevent this class of errors can dramatically affect the complexity of the I&C architecture. In some regulatory environments, the view is that human operators in the control room, more times than not, represent the major source of operational error. As a result, architectures have been designed that contain "limitation" systems intended to monitor human control actions and thwart or limit any actions that are detrimental to plant safety. Typically, such systems are functionally placed between the control system and the protection system to reduce challenges to the protection system.

Other regulatory cultures consider "common cause" the major source of error. The humans that erred are the designers/implementors, and the result of their error is common across redundant systems and devices, such that an entire function is lost or made inoperable. This has imposed the need to design and implement diverse means for accomplishing some or all safety tasks. Some cultures have taken a "belt and suspenders" approach so that the complexity of the I&C architecture is often increased to address both views.

The consequence of added systems and devices driven by some regulatory authorities and tradition, in the interests of improved safety, is to add levels of equipment actuation within the operating margin between the plant's designed "normal" operating condition and the ultimate process equipment design limits. These additional levels of equipment add complexity to the I&C design and operation. In addition, operation set points for these added systems and devices tend to eat away at the plant's operating margins and, unless carefully designed, can make normal operations and expected transients economically taxing by challenging these additional safety-related systems when they are not required.

5.1.1 Safety System Architectures

All of the evolutionary designs include functional diversity and defense-in-depth in the microprocessor architecture within each safety division. However, the approaches to achieving separation varies significantly as a result of the degree to which separate microprocessors share process input electronics and computer resources.

If properly engineered, the inclusion of a computer-based tester in the reactor protection system design can be a very comprehensive method for performing regular proof testing of the safety functions. In some countries, the need to include the feature is driven by licensees who need it to address operational test requirements, so the feature is not included in all evolutionary systems. The approach can eliminate potential common-cause errors of previous designs because the testing does not require manual reconfiguration of the protection system circuits. For example, the first version of SPIN required external cable reconfiguration to perform the regular proof testing, but the N4 SPIN version improved the design so that cable reconfiguration is no longer required.

5.1.2 Control System Architectures

The different configurations for the evolutionary designs are based on the plant instrumentation configuration, national culture, commercial arrangements, and a view (by some) that NSSS controls need to be of higher integrity than other plant process controls. The most reliable of these configurations include NSSS controllers that have redundant computer and I/O resources

to meet single-failure requirements. Most evolutionary plant control systems do not completely satisfy this requirement, in that they usually employ their standard control system redundancy configurations, which share computer resources and/or process variable I/O circuits.

5.1.3 System and Human Interfaces

Digital computer-driven human interfaces are currently in their infancy. For most of the evolutionary I&C designs reviewed, the human interfaces are barely more than computer implementations of analog interfaces and P&IDs.

For some evolutionary designs, advanced human interfaces as part of the HMI were the primary regulatory concern. The most significant regulatory issues concerned the possibility of increasing human error rates to errors in advanced operator support systems. For example, one evolutionary design incorporates computerized operating procedures, including emergency procedures, that could lead an operator to an incorrect part of a procedure if the system was to fail. Another advanced human interface is designed to reduce the operators' workload by suppressing redundant alarms using a sophisticated abnormal message logic. However, if this system does not work as designed, it could suppress alarms that the operators need to effectively respond to the event and validate automatic system responses.

Databases associated with the human interface portion of the I&C design are large and complex. Modern HMI systems use sophisticated state of the art computer graphics and methods to synthesize information for the operator. This requires significant computational power

Currently, no regulatory agencies have approved a design for Safety Class 1E soft controls (i.e., those that are displayed and activated by the VDU). In most cases, this has led to the installation of discrete controls in addition to soft controls. However, having two sets of controls exacerbates the problem of control signal priority resolution within the I&C design, adds to operator training and operating procedures costs, and increases the need for physical space on the control room panels.

As is the case with the required plant process scope of the diverse protection system, vast differences of opinion exist within the regulatory agencies around the world as to the scope of backup necessary for the use of soft controls in nuclear power plants. The notion of system-level verus component-level actuation is symptomatic of these differences.

A similar argument is ongoing about the need for a minimum inventory set of process variable indications that are to be displayed in a diverse manner. This is beyond, yet, intertwined with, the requirements already in place for post-accident monitoring. Computer-based design and configuration management tools are essential to the economical design and maintenance of the computer-based human interfaces.

5.1.4 Dependability Features

Software-based digital systems are more complex than systems based on conventional analog technology. Nevertheless, operational experience shows that, when properly engineered, software-based systems are as or more reliable as the conventional systems they replace. However, software-based digital system can have different failure modes. The primary concern has been that software common mode failure can be a significant failure mode and can defeat the diversity and defense in depth features of the protection and control system. When designing or reviewing these systems, the complexity of the overall design solution should also be considered. The case for protection system diversity and defense-in-depth must be made in conjunction with the nuclear plant safety case taking into account all plant-specific factors. For example, the Temelin common cause failure diversity requirements led to the need for a complete system, besides the two diverse systems. The AP600 DAS is an example where the design flexibility afforded by a non Class 1E diverse system can lead to a significantly less complex solution.

In the United States, a structured qualitative methodology for analyzing diversity and defense-in-depth is employed. This approach evaluates the reactor protection system design vulnerability with respect to common cause failure. The methodology identifies several types of diversity that can be employed in the analysis (i.e., human diversity, design diversity, software diversity, functional diversity, signal diversity, and equipment diversity). The regulatory authorities in other countries, such as France and Japan, impose requirements for addressing common cause failures in microprocessor-based designs that are similar to 10 CFR Part 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light Water Cooled Nuclear Power Plants." Other countries have developed more prescriptive requirements. The Czech Republic specifically requires that the reactor protection system be comprised of two separate Class 1E parts. Each part must be capable of terminating and mitigating frequent design basis events (i.e., those with a probability of occurrence greater than 1 in 1000 per year) concurrent with a postulated common cause software failure in either part, but not both simultaneously. The requirement resulted in a very complex software-based reactor protection system design. The view in the UK and with the regulatory agency in particular, is that as the level of claimed reliability increases, the demonstration of freedom from common cause failures becomes progressively more difficult. The UK regulatory position is that currently available methods are not capable of providing adequate demonstration below the 10^{-5} failures per demand level.

The issue of software common cause failures and diversity and defense in depth requirements is also an issue in the ability to risk inform current regulatory requirements. As the countries that have more quantitative reliability requirements have seen the inability to demonstrate compliance with high reliability requirements can result in more complicated solutions. As a result improvements in digital reliability methods will potentially be of significant benefit to vendors, in that it will permit less complicated and expensive solutions to this requirement. This will need to be closely monitored by the regulatory agencies, so that they are prepared to review alternate solutions to diversity and defense and depth requirements.

5.2 Field Devices

Sensors used to measure PWR Safety Class 1E variables required for the reactor protection system are a mature technology. Some sensor types that provide new methods for measuring the operation of the NSSS are beneficial because they provide additional sensor and functional diversity. The power range monitor and reactor coolant pump speed sensors are examples of such sensors. Multi-section ex-core neutron flux detectors are based on the same technology as the previous design, but the extra detectors provide more information.

5.3 Communications Technology

The hierarchal arrangement of communications networks is based on the technology available in the 1980s and early 1990s. These networks can accomplish the required function, but the performance is sometimes marginal. The performance deficiencies were addressed by adding networks to achieve the needed bandwidth. However, this approach significantly increased the complexity of the communications design.

Evolutionary plant communication installations require restructuring or creation of data records as data passes through layers of the communications network hierarchy. This presents the following difficulties:

- Restructuring or creating data records adds to the response time.
- Restructuring or creating data records adds to the software engineering design and maintenance efforts.
- Restructuring or creating data records is a source of error in software engineering and maintenance.
- Some data attributes, such as time tags, may not be instantiated in all data records because the desired information is not available from all parts of the system.

5.4 Digital Platforms

Operational experience with digital platforms in the evolutionary nuclear plants has been very good. The operational experience to date has shown that this trend is beneficial. In the U.S application-specific integrated circuits (ASICs) have not been proposed for any RPS replacements to date. Research and applications in other industries as well as in evolutionary nuclear plants indicate that functions once done in software are being absorbed into ASICs. For ASIC applications, the functions are more likely to be treated as hardware instead of software, with greater confidence attributed to the completeness of analysis results. Expected steps in the movement to fully ASIC-based protection functions may include embedded operating systems and library computational functions such as lead/lag, for future digital platforms.

5.5 Software

5.5.1 Life Cycle Approach

None of the software life cycles chosen for the evolutionary I&C designs reviewed in this study has been completed. These digital I&C designs are still in operation today. The experience to date is from that portion of the life cycle that deals with the design, construction, and installation of the software. In addition, reporting of software operational and maintenance experience has been limited.

The most common software life cycle approach is the waterfall model, which assumes that the life cycle phases (requirements, design, implementation, etc.) are continuous processes that are revisited any time software requirements are modified. While attempting to reduce errors and provide high-quality software, the waterfall model does not fully guarantee that the resulting software will be totally error-free under all possible operating conditions. The impact of this fact has been appreciated and accounted for only in the later evolutionary I&C designs. The realization that some errors may still be present in the software has prompted regulators and concerned vendors to include some form of diverse protection system, but often of limited scope.

To date, the large quantity of software produced for these evolutionary I&C designs has performed well, and no known abnormal plant events have occurred as a result of software errors. Complaints about the life cycle processes primarily have focused on the time, manpower, and documentation required to develop the software in accordance with the life cycle processes.

5.5.2 Languages

Most evolutionary I&C designs use some variant of the C computer language. Overall, there were no reported problems when the C language was used. By contrast, other software languages have had various issues. For Westinghouse implementations, the choice of the PL/M-86 computer language proved to be too microprocessor-specific. Because of the limited use of this language, it proved difficult to expand its use across different applications. The lack of familiarity with the language among vendor and plant personnel also contributed to problems, such as reduced sources of support and limited data. Because of similar problems, the PL-1 and PASCAL languages have been replaced by C. ADA was adopted for use in the Temelin Class 1E diverse protection system because of its unique characteristics and its history of development and use by the U.S. Military. However, for the above-mentioned reasons, ADA will most likely not be used in future reactor designs.

5.5.3 Coding Approaches

The division of the development of executing software and plant-specific databases into separate activities has been highly effective. Each requires the application of different technology disciplines (i.e., computer science and engineering vs. plant systems engineering). The division has permitted plant staff to take ownership of the appropriate portion of the total task.

Software tools aimed at improving the productivity and quality of the initial software programming and ongoing software configuration management efforts are essential. However, the use of software tools to support extensive nuclear plant I&C system development has had mixed results. All cases they have required significant effort. A set of limited-scope tools that may be combined into an integrated tool in the future is an approach that should reduce the risk.

The creation of the plant-specific database (i.e., the offline task) for digital I&C systems is a monumental and very costly task that currently is not particularly amenable to the development and application of special-purpose, software-based tools. Little capability is available to transfer a learning curve from one plant to the next. TXS-based safety systems are created using the Specification and Coding Environment (SPACE) tool, which provides a graphical user interface for translating plant engineering data into software system requirements and design data. This data is subsequently translated into software modules that are compiled with an ANSI C compiler. Most of the SPACE work is done by Framatome personnel under contract to the licensee. Consequently, for this system development environment there is some knowledge transfer between tasks.

5.5.4 Safety System Verification and Validation

The licensing of software-based systems illustrates differences in regulatory methodologies and emphasis among countries. The primary differences result from the quantity of evidence considered necessary and the perceived quality of the evidence derived from various V&V approaches. Sometimes, additional independent V&V activities were required to satisfy regulatory concerns. The confidence contributed by such supplemental evidence could not be quantified, and the efforts proved costly and time-consuming. As a result, the principal lessons learned are that clear and consistent expectations for software V&V are still evolving. A more systematic determination of the relationship between the required evidence (e.g., type, quantity, and quality) and the necessary and sufficient confidence level is needed.

A case study of the application of software-based microprocessor technology to a reactor protection system at Sizewell B demonstrates the impact of varying international expectations and the potential for licensing inefficiency. The licensing review of the Westinghouse PPS at Sizewell B resulted in supplemental independent software V&V. One of the safety assessment principles in the United Kingdom requires licensees to undertake adequate peer review and independent assessment of their safety cases. Therefore, the PPS design was reviewed first by the licensee (British Energy) and then by the NII.

The software assessment performed by British Energy was separate from the Westinghouse independent verification based on accepted U.S. nuclear industry standards. The review was done, in part, through contracts with various outside groups. The British Energy software assessment consisted of a "fitness for purpose" review and additional confirmatory assessments that used techniques to impose formalism on the assessment process. Because the British Energy confirmatory V&V activities took place after the completion of the Westinghouse IPS/PPS design and verification, it was also a check of the Westinghouse verification process, as well as corroboration of the design implementation. No findings arising from the British Energy confirmatory activities resulted in software modification for the safety-

critical functionality of the system; that is, the system could trip the reactor and initiate safety equipment when required.

During the Sizewell B licensing process, software experts raised several issues, including concerns from the internal review and from external interested parties. Specifically, the software experts expressed concerns about the use of the PL/M-86 language, and some reviewers felt that PASCAL would perhaps have been a better selection. After a consensus was finally achieved that PL/M-86 was a suitable structured language, the reviewers raised concerns about the capability of a unique language such as PL/M-86 to produce error-free executable code. However, it was the designer's position that the widespread use of a particular compiler, not the language, leads to confidence in the fidelity of the executable code. Nevertheless, to address this concern, a decompilation verification was performed and no problems were discovered.

Additionally, the reviewers raised a concern about the PPS software size. The reasoning behind this concern derives from the thought that a monolithic subsystem software approach would be shorter and, therefore, simpler than that achieved by a structured modular software design, where software modules are intended for use in many subsystems and systems. In addition, it was argued that such an approach, where each subsystem has completely separate code, would be less prone to common-mode failure. The designer's position was that, while a single subsystem would have smaller code size, the code for the entire system would be larger. Moreover, approaches to common-cause failure are generally subjective, and the design approach that stressed reuse to gain maximum operational experience was an equally valid approach. The Westinghouse position was accepted.

Next, the reviewers expressed concerns regarding the use of indirect addressing, which was necessary to meet several PPS software design principles. For example, the separation of code and configuration data provide for reusable software modules to allow microcomputers to have the same software across the entire system and thus be treated like other replaceable hardware modules. In addition, the separation of the code and calibration data allows calibration data adjustments to be performed without reverifying the code. The concern was exacerbated because pointers associated with some indirect addressing were located in random access memory (RAM) due to a limitation in the PL/M-86 compiler. Some reviewers viewed RAM as having lower integrity than PROM, despite its inclusion in the self-diagnostic regimen. The software tool could not analyze this software configuration automatically, so the consulting software team used software inspection to conclude that no threat condition existed.

5.6 Information/Data Management

From the point of view of data management, other than the broadcast of real-time data records, little management of the data occurs in current distributed digital control and supervisory systems. The software architecture for data processing and plant supervision is usually based on a set of monolithic subsystems connected by a control data network that exchanges plant process data among the subsystems. Very little data is communicated among these individual systems about their computational results. Essentially, these systems listen for new process data, perform their calculations, and make that data available for VDU display. This is the combined result of the limited capabilities of the communications technology that was available

in the late 1980s and early 1990s implementation approach, which was prevalent for most I&C upgrades. So far, emphasis is limited to the control portion of the distributed digital control and supervisory systems.

Evolutionary designs use two approaches for plant alarms. One approach includes the alarm state and associated alarm data as fields or attributes of a real-time data record structure. The other approach treats the alarm as a separate synthetic variable. Each approach has benefits and deficiencies ,and the correct selection depends of the operation of the alarm system. Some solutions, such as the Beznau alarm system, use both approaches within one system. This causes potential conflicts, which can be left to the control room operators to resolve in real time.

5.7 Testing Approach

Since the Three Mile Island Unit 2 incident, the use of plant-specific operator training simulators for all of the Western-style commercial nuclear power plants has become the accepted practice. This situation includes the development of validated computer modules for most commercial nuclear power plants. To meet the requirements of operator training, these models operate in real time. Portions of some evolutionary plant I&C designs were developed and/or validated using test equipment designed to employ these models.

While the use of simulators for system validation testing yields good results, the costs of some of these efforts causes concern in some applications. The development of the Sizewell B primary protection system test harness, which was based on Sizewell B simulator models, was an expensive exercise.

The NOK ANIS project was the first of these evolutionary I&C designs to use simulators in the manner advocated by EPRI ALWR Utility Requirements Document. A single complete train of the NOK ANIS evolutionary I&C hardware, including the software and plant-specific databases, was set up in the computer room of the NOK Beznau crew training simulator. The simulator plant process models developed simulated plant process signals that were then sent to the ANIS hardware to simulate its operation. Operating crews were then given plant transients and operational problems that, in the end, provided validation of the *entire* system (i.e., the system's hardware, software, and databases, as well as the human operators who must work in real time with that hardware and software). In addition, it gave the operators training on the new computerized HSI. This configuration has remained, permitting Beznau personnel to make any needed changes to the plant-specific databases, validate those changes, and familiarize the operators with the changes before they are implemented.

5.8 System Performance

A large and robust I&C system is required to meet the needs of nuclear power plant protection, control, and supervisory functions. With respect to data throughput for the supervisory and data management functions that have been put into operation to date, the evolutionary designs demonstrate marginal performance, as illustrated by the following examples:

- The N4 data management, complex data processing, and human system interfaces are based on late 1970s and early 1980s computer technology. This has limited the capabilities of the N4 systems.
- The Beznau NOK ANIS required additional data networks dedicated to particular functions (such as the alarm system).
- Little capacity margin exists for additions to the Sizewell B non-Class 1E data networks. The data networks that broadcast plant process variables for plant supervision have to be carefully monitored when changes or additions are made.
- The Temelin I&C architecture uses a high-performance data network for plant supervision. However, in the Temelin layered network design, certain functions (such as the manual control function) have marginal performance. In addition, new requirements on the network from the diagnostic and monitoring system and other systems take up a significant portion of the network bandwidth.
- The ABB Advant system applied to the Oskarshamn Unit 1 BWR has high-performance microprocessors but medium-performance data networks. Moreover, the non-Class 1E control network is based on the Ethernet protocol. The network performance is marginal for a nuclear power plant.

6. ANTICIPATED NEW ISSUES

The I&C systems envisioned for the nuclear reactor concepts under consideration for near-term deployment, which are primarily derived from ALWR designs, are very similar to those implemented at evolutionary nuclear power plants. However, the International Near-Term Deployment (INTD) and Generation IV reactor concepts may pose some new issues that need to be considered in establishing an effective and efficient licensing regime within the United States. Principally, the modular reactor configurations, such as the International Reactor Innovative and Secure (IRIS), the PBMR, and the GT-MHR, may introduce unique considerations regarding phase commissioning of modules, common control rooms and/or auxiliary systems, and shared site operations and maintenance functions. Because the modular plant designs have not definitively established the full scope of "modularity," it is difficult to predict the specific issues that may arise. However, consideration of the potential impact of various approaches to building a modular multi-unit plant is necessary to prepare for the review of future license applications. This section discusses some of the relevant issues.

The evolution of I&C technology may also pose new issues for review and evaluation as new capabilities and different performance characteristics emerge. Examples would include radiation-hardened electronics that permits microprocessor-based implementations within containment and wireless communications networks that can reduce cable installations and increase bandwidth. The prospects for the introduction of emerging technologies to nuclear plant safety-related I&C systems are presented in detail in NUREG/CR-6812, "Emerging Technologies in Instrumentation and Controls." In addition, NUREG/CR-6812 discusses the potential research needs arising from those technologies. This information is not repeated in this report.

Finally, the development of reactor concepts outside of the traditional light-water experience may alter the context for licensing safety-related I&C systems, which may be required to withstand environmental conditions that are more extreme than those experienced by conventional design. The evolutionary designs may also experience different safety demands associated with unique design-basis events and potentially more forgiving nuclear systems. Because the issues related to the nature of the innovative nuclear systems are more properly covered in the broader scope of establishing the overall safety case for those reactor concepts, and because the issues would be unique for each INTD and Generation IV concept, they are not be explicitly treated in this text. However, the issues of multi-module construction and environmental conditions are discussed below.

6.1 Multi-Module Construction Sequencing of I&C Systems

While multiple-module operation of any reactor systems is an option, it has been explicitly included in the design of the gas reactors and the integral PWR with multiple smaller units making up approximately 1,000 MWe output from a single site. For both the pebble bed and prismatic block designs, a common plant-wide control architecture is employed on the non-Class 1E monitoring systems. This plant-wide data network addresses the specific module operating systems and essential plant-wide auxiliary systems shared between all the units. The control design allows a control operator to operate a single unit in a shared control complex.

The challenge is to address operability issues of the shared and common systems when the first module is declared operational and the follow-on modules are still under construction. Because of the advances in I&C technology, common data networks that transmit and utilize large amounts of information will serve as integrated data links rather than the traditional direct point-to-point wiring. Thus, the control and monitoring operations of these modules must be fully operational and not susceptible to interference from construction and testing activities in the non-operational modules. Research is needed to address basic guidelines that may include modifications to the data highway and control room design to optimize the construction sequencing. This may result in a control room that is less optimal for human factors at all levels than would otherwise be possible if all the modules simultaneously completed construction. In addition to licensed operation, an option to consider is the use of a dedicated commissioning room in which a module would be commissioned and then "transferred" to the shared control room.

6.2 Environmental Qualification

Qualification of instrumentation for applications in either gas reactor design (pebble bed or block) presents significant challenges, which should be addressed through both short- and long-term analysis and testing. This new qualification process needs to address whether existing qualified instrumentation used at light-water reactors can be expanded so that it can be used for gas reactor applications, or whether new classes of instrumentation will be necessary. In either case, the instrumentation must be qualified in accordance with IEEE-323 for environmental qualification and IEEE-344 for seismic qualification, along with the associated NRC regulatory guides and applicable sections of the standard review plan. This qualification will require a revised hazards profile over time, consisting of temperature, pressure, chemical spray, and other environmental stressors. The peaks and variation over time for temperature and other environmental stressors are clearly different for gas reactors and may require significant changes and testing to verify that the environmental envelope bounds all of the accident scenarios that will be part of the reactor-specific safety analysis.

In moving forward for the gas reactor designs, initial studies have shown the following challenges to environmental qualification for the gas reactor instruments:

- Find accurate helium flow meters for the high-temperature and high-pressure environment. These measurements are required to calculate fluidic power and to thermally correct the neutron instrumentation systems. The flow meters will not be safety-related, but will operate at 500°C and 8300 kPa in the pebble bed design. The equivalent system design for the prismatic block design has not yet been defined. Accurate flow meters will largely determine the maximum power setting for plant operation.
- Find small neutron detectors, especially source range detectors. These detectors need to be embedded in the core reflector for reactor control during startup and will remain functional in the temperature ranges around 500°C.

7. CONCLUSIONS AND RECOMMENDATIONS

Experience with advanced I&C technologies at evolutionary nuclear power plants has shown that safety-related systems can be developed and licensed for commercial nuclear power plants. However, as shown by the evidence documented within this report, licensing issues have arisen and some design and performance issues have been experienced. Many of these issues can be attributed to uncertainties regarding the safety significance of unique physical, functional, and performance characteristics introduced by new technology. Existing requirements and regulatory guidance are focused on current generation plants, and they have a tendency to be prescriptive with assumptions about particular design approaches. As a result, the introduction of advanced I&C technologies has prompted reassessments, enhancements, and development of regulatory positions to address these issues.

Although several new or unique I&C systems and methods will be used in advanced reactors, many of these will not be of regulatory concern. Additionally, the current review methods may be adequate for the review of many of these new technologies. However, as the National Research Council study noted, the NRC's regulations and review methods may unnecessarily limit new design features or prove difficult to implement for new technologies or plant applications.

The primary recommendation of this report is that the NRC should review its current regulations in several areas to determine whether revisions may be needed in either the regulations themselves, or the appropriate regulatory guidance found in the standard review plan, regulatory guides, and BTPs. Specifically, the NRC should consider the following areas:

- main control room design reviews
- human system interfaces
- displays and soft controls (RG 1.47)
- post-accident instrumentation (RG 1.97)
- alarms
- system isolation and cyber security
- system architecture
- network communications
- software common-cause failures
- redundancy, diversity, and defense in depth
- sensors
- information and data management
- software tools, including change control and security
- system reliability
- commercial off-the-shelf (COTS) systems

These and other issues are of concern in the design, construction, and licensing of the evolutionary plants and may be issues for the NRC in the licensing of the next generation of U.S. nuclear power plants.

Specific recommendations for research to support the reviews suggested above are given in the following sections according to topic.

7.1 I&C System Architectures

The use of high-bandwidth communications technologies, such as fiber optic data links, facilitates the transmission of extensive quantities of data from plant safety systems to other non-safety systems such as control, surveillance, and plant information systems. This data can yield significant operational and safety-related performance benefits. However, this communication capability can introduce functional coupling between safety and non-safety systems. While it is usually best for the safety system to perform only computations that are directly associated with the safety functions, some non-safety function computations(e.g., time-tagging) can only be performed, or are best performed, in the safety system. Research to develop the technical basis for guidance in this area would be useful. One element of such research could be a detailed study of the tradeoffs in evolutionary nuclear plants between benefits derived from equipment added to improve safety and the impact on plant safety margins.

With distributed digital I&C designs that contain multiple communications networks and/or complex, time-consuming calculations, the time coherency of the data provided to automatic systems and the presence of control room operators can no longer be assumed. Nuclear power plant I&C architecture designers have paid little attention to this issue in the past. As a result, no standard techniques exist for establishing and confirming the time coherency of data, and there are no standard criteria for acceptable tolerances of non coherence. The NRC has conducted research regarding data sampling rates for digital applications, but further investigations are warranted to determine the time coherency characteristics of distributed digital systems.

The desire to extract data from the nuclear plant I&C system to support and automate enterprise management functions raises issues of data control and integrity, as well as the security of the safety function. If such communication connections are established, measures must be taken to ensure that plant safety cannot be adversely affected by either accident or sabotage. Ongoing research into cyber security should continue to establish guidance on effective design and implementation practices and approaches that will confirm and maintain cyber security.

7.1.1 Safety System Architectures

Increased microprocessor performance enables more compact reactor protection system implementations. Thus, current safety system configurations, which are based on extensive internal diversity and defense-in-depth, may be condensed in future implementations through increased functional density. Two key points are associated with this potential research topic. First, if licensees or vendors do not receive credit for the full range of architectural features in present designs, they will be motivated to cut costs by collapsing features into a more compact architecture. If credit is then given for diversity and defense-in-depth within a single safety system channel, guidelines should be established for internal separation throughout the channel. The following questions must then be addressed:

- Are diverse functions permitted to share common signal conditioning electronics?
- Are multiple microcomputers containing diverse functions permitted to share a common computer bus or a common data network?

- Are safety divisions permitted to share a common fiber optic data network?

These considerations should be investigated to determine their potential safety significance and to develop the necessary technical bases for guidance.

Operational and safety benefits can be associated with incorporating regular proof testing of safety functions within the safety system design. However, accommodating dynamic testing leads to design considerations that warrant study. This research should address the following questions:

- Is safety software permitted to alter its input or output data path during the test period to accommodate the test regime?
- Is it permissible to test a representative function of a similar functional grouping rather than routinely testing all functions?

The technical basis for dynamic testing guidelines should be established to address this design feature.

Including hardware diagnostics in the software design has shown to be an effective method to quickly identify random hardware failures, thereby providing a positive impact on plant safety and availability. However, analysis and test methods that would verify that the hardware diagnostics are comprehensive are needed. Although data from operating experience is sparse, some compilation of available data might provide additional insight into the effectiveness of different techniques.

7.1.2 Control System Architectures

Evolutionary plants use automated control over an extensive operational range and utilize surveillance and diagnostic systems to contribute to operational and maintenance decisions. Increased automation and the advent of autonomous control capabilities present the opportunity to improve the operational performance of advanced nuclear power plants and to reduce the prospect for human error challenging a safety system. However, the assumption of decisionmaking responsibilities by the computer systems expands the need for highly reliable software and raises the issue of the fidelity of the surveillance and diagnostic information upon which decisions would be based. Research issues that should be considered include the role of the human in plant operations, the potential safety significance and quality requirements for control systems that assume a greater role in the planning and management of the plant, and the uncertainties inherent in diagnostic/prognostic techniques.

7.1.3 System and Human Interfaces

There is a need for systematic determination of the requisite attributes of computer-based support tools and databases that can contribute to safety. This evaluation should have two elements. First, determine the capabilities or attributes that have a safety benefit. Second, determine the capabilities or attributes that can have an undesired safety impact. Detailed evaluation of experience from evolutionary plant implementations and confirmatory research using laboratory demonstrations can support the identification of desired attributes and help establish guidelines on design and implementation of these types of information systems. In

addition, an assessment is needed of the demands that improved human-system interfaces impose on the design of distributed digital I&C systems and the impact of those design changes on the safe operation of the plant.

7.1.4 Dependability Features

For advanced plants, the practice of imposing a diverse and independent means of implementing a safety function should be carefully considered in terms of the overall reliability of the reactor protection system to ensure that neither unnecessary complexity nor an undesired safety impact is introduced. To keep the overall system design as simple as practical, the type, or class, of common-cause failures should be identified early in the design process. Research should be conducted to develop the technical basis for guidelines for performing these evaluations. An element of this research could be a detailed study of the consequences of the evolutionary plants' "risk-based" (e.g., Sizewell B), "risk-informed" (e.g., AP600), and "deterministic" (e.g., Temelin) approaches. This will be particularly important as the NRC moves forward in its development of the risk-informed future reactor licensing framework.

Developing a completely failsafe reactor protection system design is probably not possible. Nevertheless, failsafe design attributes can improve protection system dependability. Therefore, the NRC should establish the technical basis for guidance for evaluating the effectiveness of various failsafe approaches in a reactor protection system design. This guidance should consider the feature as a defense against common-cause failure.

7.2 Field Devices

For light-water reactor technology, the evolutionary digital I&C designs have not revealed any new regulatory issues about Safety Class 1E sensor technology. However, significant research has been conducted toward improving sensor technology that will probably have application and be cost-effective in commercial nuclear power plants. In addition, new sensing systems, unique measurement parameters, and environmental compatibility under more extreme conditions may be required to support other advanced reactor designs. As a result, a research program to support licensing of future plants should consider maintaining an ongoing awareness of such developments and determining the viability of such improvements to nuclear power plant applications.

7.3 Communications Technology

Communications technology may have the most significant impact on nuclear power plant I&C systems of any technology since the introduction of the microprocessor. Research can contribute the technical basis for guidance on the application of advanced communications technology for safety-related I&C systems. In particular, this research should address issues such as separation, isolation, redundancy, topology, predictability, timeliness (or lag time), and data transmission/reception consistency throughout the communications architecture. The scope of communications guidance should include the safety, automation, and human interface portions of the safety-related I&C system in a nuclear plant.

Although enhanced sensor network functionality may increase the design complexity for Class 1E applications, safety-class versions of field device communications architectures are under development and safety-related application of such networks seems likely for future nuclear power plants. Therefore, the NRC should conduct a study of the safety characteristics of various fieldbus network approaches.

7.4 Digital Platforms

A current issue surrounding analog I&C systems is equipment obsolescence. The pace of technology advancement for microprocessors is much more rapid than that of analog technologies. As a result, it will be problematic to maintain a product line using a digital platform based on a particular generation of microprocessors over an extended period. Consequently, the NRC should conduct research to develop guidance to address issues associated with platform obsolescence. For example, the design and performance characteristics must be determined to establish the equivalence of same-generation versions of microprocessors or subsequent generations of microprocessor families.

7.5 Software

7.5.1 Life Cycle Approach

Given the costs of the software life cycle process used by the nuclear industry and the qualitative nature of the evidence generated, a need exists for periodic reviews of the state-of-the-art to maintain an in-depth awareness of developments in the software engineering discipline. These state-of-the-art reviews are particularly important because they affect the productivity of software engineers and the development of effective, efficient processes for the design and maintenance of high-integrity software. In particular, the NRC should pursue research regarding measures of the effectiveness of life cycle approaches to establish quantitative evidence of expected software quality and to provide the basis for optimizing the activities that are necessary over the software lifetime. In addition, the NRC should follow the recent trends toward the use of "object-oriented" software design, reusable code, and domain engineering.

7.5.2 Languages

The NRC has previously conducted research to evaluate the safety aspects of various languages and coding structures. However, it would be beneficial to maintain awareness of any emerging trends or developments. This is particularly true with regard to evaluating the selection of alternative languages for diverse implementations to address potential common-cause failures. Thus, it could prove valuable to conduct a periodic review of the application of formal methods in high-integrity military applications.

7.5.3 Coding Approaches

Currently, little guidance is available for software-based development tools and code generation approaches, particularly those used to build and maintain databases. Since these tools are

usually used for a wide variety of coding for both generic and plant-specific implementations, they present a potential for introducing common-mode faults. Research is warranted to investigate and classify potential sources of errors from their use and to contribute to standards for software-based development tools. The NRC should also establish a basis for evaluating the safety significance of the use of such tools in the design, construction, and maintenance of both online and offline executing code and databases.

7.5.4 Safety System Verification and Validation

Because of the process-oriented, qualitative nature of the V&V process for software design and implementation, development has focused on diversity to provide acceptably reliable safety system software. However, a consequence of this approach is a more complex overall design for reactor protection systems. Research should continue to investigate methods and measures to quantify software dependability. A main consideration in the use of formal methods for software development is the assertion that such software is mathematically "proven" correct. The NRC should develop a benchmark employing a test case suite, to evaluate the capability of various methodologies, and that suite should contain complex real-time software structures inherent to reactor protection system software. The value would be an understanding of the confidence levels that can be established for software and the potential for less complex reactor protection and I&C system architectures.

7.6 Information/Data Management

Given the discrete nature of digital data and the distributed nature of digital data acquisition and computational systems, careful analysis is required to verify the claims of different time-tagging schemes. Consequently, the NRC should conduct research to identify the potential safety-related issues that could arise from different approaches. The NRC should also develop the technical basis for evaluating time-tagging methods.

The technology for evaluating the quality and effectiveness of a functionally distributed software architecture within a physically distributed digital hardware architecture is currently in its infancy. Thus, the NRC should monitor emerging trends and conduct research to identify and evaluate the safety attributes associated with the prominent software architectures.

7.7 Testing Approach

The use of simulators for system functional validation is one of the more novel and powerful design and testing approaches used for I&C systems at evolutionary nuclear power plants. A detailed investigation of the industry's specific experiences with this approach could better characterize its potential value and identify any issues of concern (e.g., level of simulation fidelity, impact of unmodeled dynamics). This study was necessarily limited as a result of restricted access to detailed information. An additional area of research arises from software testing. In addition, the NRC should investigate issues of fault seeding and detection limitations, the statistics of rare events, and usage modeling for test management to develop the technical basis for guidance where warranted.

7.8 System Performance

No specific requirements exist for the time responses required for protection, control, and supervisory portions of the nuclear I&C system. This lack of requirements is a legacy from conventional technology, where the response time for protection and control was considered instantaneous and the computer functions were not as important. In addition, no standards exist for confirming these numbers. For example, no standard is available to determine whether worst case or statistical methods should be used, and no guidance is available on testing to support analytical results. Consequently, the NRC should consider research to develop the technical basis for guidance on defining the necessary time response requirements, acceptable methodologies for developing the requirement, and acceptable methods for confirming the actual time response.

8. BIBLIOGRAPHY

C. Chun, L. Staples, and A.J. Faya, "Regulatory Assessment of the Darlington Shutdown System Trip Computer Software Redesign," *Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Washington, DC, November 2000.

M.P. Feher, E.C. Davey, and L.R. Lupton, "A Design Basis for the Development of CANDU Control Centers," *Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Pennsylvania State University, Pennsylvania, May 1996.

A. Faya, L. Tougas and R. Taylor, "Regulatory Assessment of Upgrades to Digital Systems," IAEA Technical Committee Meeting, Helsinki, Finland, June 1994.

IAEA Workshop/Specialists Meeting on Approaches for the Integration of Human Factors into the Upgrading and Refurbishment of Control Rooms, Halden, Norway, August 1999.

A. Faya, R. Taylor and L. Tougas, "Specifying Requirements for Safety Systems," *Proceedings of the Institute of Mechanical Engineers (U.K.) Nuclear Power Safety Standards: Toward International Harmonization*, London, England, October 1993.

"Four Party Regulatory Consensus Report on the Safety Case for Computer-Based Systems in Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC, November 1997.

M. LaBar, "The Gas Turbine-Modular Helium Reactor: A Promising Option for Near-erm Deployment," *Proceedings of the ANS Annual Meeting*, Hollywood, Florida, June 2002.

C. Rodriguez, D. Pfremmer and A.J. Neylan, "The Gas Turbine-Modular Helium Reactor: Simulator Supports Paradigm Shift," GA-A21784, General Atomics, San Diego, California, August 1994.

C. Rodriguez, J. Zgliczynski and D. Pfremmer, "GT-MHR Operations and Control," GA-A21894, General Atomics, San Diego, California, November 1994.

E.L. Quinn and C. Rodriguez, "The Gas Turbine Modular Helium Reactor, Optimum Design for Instrumentation and Control," *Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Washington, DC, November 2000.

K.J. van Rensburg, and J. Hugo, "Pebble Bed Modular Reactor Automation System," May 2002, available at http://www.orau.gov/icandhmiworkshop/.

International Conference on Electrical and Control Aspects of the Sizewell B PWR, Power Division of UK Institute of Electrical Engineers, Cambridge Conference Publication 361, September 1992.

World Technology Evaluation Center Panel Report on European Nuclear Instrumentation and Controls, Loyola College, Baltimore, Maryland, December 1991.

Japan Technology Evaluation Center Panel Report on Nuclear Power in Japan, Loyola College, Baltimore, Maryland, October 1990.

G.W. Remley, "Distributed Digital Processing Technology Applied to Commercial Nuclear Power Station Controls," UK Institution of Mechanical Engineers, Manchester Conference Publication C388/014, September 1989.

H.K. Hajek, et al., "Dynamic Safety Systems for BWR Reactor Protection System Upgrade," *Ninth Power Plant Dynamics, Control, & Testing Symposium Proceedings*, Knoxville, Tennessee, May 1995.

A.C. Kauffman, et al., "Emulation of a Dynamic Safety System Reactor Protection System for a US Light Water Reactor," *Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies*, Pennsylvania State University, Pennsylvania, May 1996.

CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems: Workshop Proceedings, NEA/CSNI/R(2002)1/VOL1, Organization for Economic Cooperation and Development, Nuclear Energy Agency, June 2002.

CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems: Workshop Proceedings, NEA/CSNI/R(2002)2/VOL2, Organization for Economic Cooperation and Development, Nuclear Energy Agency, June 2002.

Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies, American Nuclear Society, Pennsylvania State University, Pennsylvania, May 1996.

Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies, Washington, DC, November 2000.

Proceedings of the ANS Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies, Oak Ridge, Tennessee, April 1993.

R.W. Winks, T.L., Wilson, and M. Amick, "B&W PWR Advanced Control System Algorithm Development," *Proceedings of the Conference on Advanced Digital Computers, Controls, and Automation Technologies for Power Plants*, EPRI TR-100804, Electric Power Research Institute, Palo Alto, California, August 1992.

"Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants," IAEA-TECDOC-1327, International Atomic Energy Agency, Vienna, Austria, December 2002.

Proceedings: Licensing Digital Upgrades for Nuclear Power Plants, EPRI TR-104600, Electric Power Research Institute, Palo Alto, California, December 1994.

Proceedings: Distributed Digital Systems, Plant Process Computers, and Networks, EPRI TR-104913, Electric Power Research Institute, Palo Alto, California, March 1995.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-6842
ORNL/TM-2004/74

2. TITLE AND SUBTITLE

Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants

3. DATE REPORT PUBLISHED

MONTH	YEAR
April	2004

4. FIN OR GRANT NUMBER

Y6478

5. AUTHOR(S)

R. T. Wood, S. A. Arndt (NRC), J. R. Easter (Preferred Licensing Services), K. Korsah, J.S. Neal, E. L. Quinn (Longenecker & Associates), and G. W. Remley (Consultant)

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

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

Preferred Licensing Services
P.O. Box 14431
Pittsburgh, PA 15239-0431

Longenecker & Associates
P.O. Box 3094
Del Mar, CA 92014-6904

205 Harrow Drive
Pittsburgh, PA 15238-2530

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Engineering Technology
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555-0001

10. SUPPLEMENTARY NOTES

Steven A. Arndt, NRC Project Manager

11. ABSTRACT *(200 words or less)*

This report presents the findings from a study of experience with digital instr umentation and controls (I&C) technology in evolutionary nuclear power plants. In particular, this study evaluated regulat ory approaches employed by the international nuclear power community for licensing advanced I&C systems and identified lessons learned. The report (1) gives an overview of the modern I&C technologies employed at numerous evolutionary nuclear power plants, (2) identifies performance experience derived from those applications, (3) discusses regulatory processes employed and issues that have arisen, (4) captures lessons learned from performance and regulatory experience, (5) sugges ts anticipated issues that may arise from international near-term deployment of reactor concepts, and (6) offers conclusions and recommendations for potential activities to support advanced reactor licensing in the United States.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Advanced Reactor, Instrumentation and Control, Digital, Software, Reliability, Lessons Learned, Emerging Technology

13. AVAILABILITY STATEMENT

unlimited

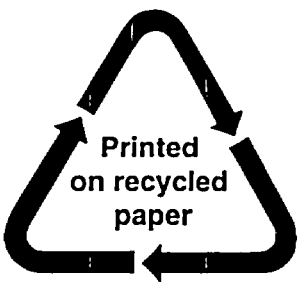
14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS