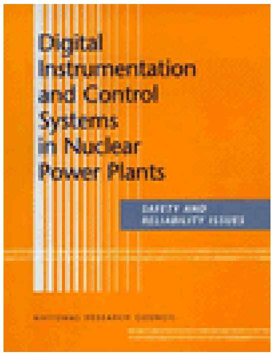

Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues

Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, National Research Council2

ISBN: 0-309-52444-X, 128 pages, 8.5 x 11, (1997)

Digital Instrumentation and Control Systems in Nuclear Power Plants

SAFETY AND RELIABILITY ISSUES

Final Report

Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety

Board on Energy and Environmental Systems
Commission on Engineering and Technical Systems
National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1997

NATIONAL ACADEMY PRESS • 2101 Constitution Avenue, N.W. • Washington, D.C. 20418

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

This report and the study on which it is based were supported by Contract No. NRC-04-94-055 from the U.S. Nuclear Regulatory Commission.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the U.S. Nuclear Regulatory Commission.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is interim president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chairman and interim vice chairman, respectively, of the National Research Council.

Limited copies of this report are available from:

Board on Energy and Environmental Systems
National Research Council (HA-270)
2101 Constitution Avenue, N.W.
Washington, DC 20418
(202) 334-3344
bees@nas.edu, http://www2.nas.edu/bees

Additional copies are available for sale from:

National Academy Press
Box 285
2101 Constitution Avenue, N.W.
Washington, DC 20055
800-624-6242 or 202-334-3313 (in the
Washington Metropolitan Area)
http://www.nap.edu

Library of Congress Catalog Card Number 97-66084
International Standard Book Number 0-309-05732-9

Printed in the United States of America.

COMMITTEE ON APPLICATION OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS TO NUCLEAR POWER PLANT OPERATIONS AND SAFETY

DOUGLAS M. CHAPIN (chair), MPR Associates, Alexandria, Virginia
JOANNE BECHTA DUGAN, University of Virginia, Charlottesville
DONALD A. BRAND, **NAE**, Pacific Gas and Electric Company (retired), Novato, California
JAMES R. CURTISS, Winston and Strawn, Washington, D.C. (from October 1995)
D. LARRY DAMON, Bechtel Research and Development, San Francisco, California
MICHAEL DeWALT, Federal Aviation Administration, Seattle, Washington (from October 1995)
JOHN D. GANNON, University of Maryland, College Park
ROBERT L. GOBLE, Clark University, Worcester, Massachusetts
DAVID J. HILL, Argonne National Laboratory, Argonne, Illinois
PETER E. KATZ, Calvert Cliffs Nuclear Power Plant, Lusby, Maryland
NANCY G. LEVESON, University of Washington, Seattle
CHRISTINE M. MITCHELL, Georgia Institute of Technology, Atlanta
CARMELO RODRIGUEZ, General Atomics Company, San Diego, California
JAMES D. WHITE, Oak Ridge National Laboratory, Oak Ridge, Tennessee

Project Staff

TRACY D. WILSON, study director, Board on Energy and Environmental Systems (BEES)
SUSANNA E. CLARENDON, senior project assistant, BEES (from May 1996)
THERON FEIST, project assistant, BEES (until June 1995)
HELEN JOHNSON, administrative associate, BEES (until July 1995)
WENDY LEWALLEN, senior project assistant, BEES (June 1995 to May 1996)
MAHADEVAN MANI, associate executive director, Commission on Engineering and Technical Systems (from January 1996)
JAMES J. ZUCCHETTO, director, BEES (from January 1996)

NAE: Member, National Academy of Engineering

BOARD ON ENERGY AND ENVIRONMENTAL SYSTEMS

ROBERT L. HIRSCH (chair), Energy Technology Collaborative, Inc., Washington, D.C.
RICHARD MESERVE (vice chair), Covington and Burling, Washington, D.C.
JAN BEYEA, Consultant, New York, New York
E. GAIL de PLANQUE, **NAE**, Consultant, Potomac, Maryland
LINDA C. DOLAN, Lockheed Martin Electronics and Missiles, Orlando, Florida
WILLIAM FULKERSON, University of Tennessee, Knoxville
JACQUES GANSLER, TASC, Inc., Arlington, Virginia
ROY S. GORDON, **NAS**, Harvard University, Cambridge, Massachusetts
FRANCOIS E. HEUZE, Lawrence Livermore National Laboratory, Livermore, California
LAWRENCE T. PAPAY, **NAE**, Bechtel Group, Inc., San Francisco, California
RUTH A. RECK, Argonne National Laboratory, Argonne, Illinois
JOEL SPIRA, **NAE**, Lutron Electronics Co., Inc., Coopersburg, Pennsylvania
JAMES LEE SWEENEY, Stanford University, Stanford, California
IRVIN L. WHITE, UTECH, Inc., Fairfax, Virginia

Former Members Active during Reporting Period:

H.M. (HUB) HUBBARD (chair), Pacific International Center for High Technology Research (retired), Honolulu, Hawaii
ROBERT D. BANKS, World Resources Institute, Washington, D.C.
ALLEN J. BARD, **NAS**, University of Texas, Austin
DAVID E. DANIEL, University of Texas, Austin
THOMAS O'ROURKE, **NAE**, Cornell University, Ithaca, New York

Liaison Members from the Commission on Engineering and Technical Systems

RICHARD A. CONWAY, **NAE**, Union Carbide Corporation, South Charleston, West Virginia
JERRY SCHUBEL, New England Aquarium, Boston, Massachusetts

Staff

JAMES J. ZUCCHETTO, director (since January 1996)
SUSANNA E. CLARENDON, administrative assistant
WENDY LEWALLEN, senior project assistant (until May 1996)
JILL WILSON, senior program officer
TRACY D. WILSON, senior program officer

NAE: Member, National Academy of Engineering
NAS: Member, National Academy of Sciences

Preface

The nuclear industry and the staff of the U.S. Nuclear Regulatory Commission (USNRC) have worked for several years on how best to safely introduce digital instrumentation and control systems into nuclear power plants. But together they have failed to reach consensus. This lack of consensus led the USNRC to request the National Research Council, through its Board on Energy and Environmental Systems of the Commission on Engineering and Technical Systems, to conduct the study whose results are reported here. The National Research Council's Computer Science and Telecommunications Board and the Council's Division on Education, Labor, and Human Performance provided additional technical support.

The Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety (see Appendix A) was appointed by the National Research Council on December 20, 1994, to examine the use of digital instrumentation and control systems in nuclear power plants. This work was to be conducted in two phases. The final report summarizes the work of both Phase 1 and Phase 2.

In Phase 1, the committee was charged to define the important safety and reliability issues (concerning hardware, software, and human-machine interfaces) that arise from the introduction of digital instrumentation and control technology in nuclear power plant operations, including operations under normal, transient, and accident conditions. In response to this charge the committee identified eight key issues associated with the use of digital instrumentation and control (I&C) systems in existing and advanced nuclear power plants. The eight issues separate into six technical issues and two strategic issues. The six technical issues are: systems aspects of digital I&C technology; software quality assurance; common-mode software failure potential; safety and reliability assessment methods; human factors and human-machine interfaces; and dedication of commercial off-the-shelf hardware and software. The two strategic issues are the case-by-case licensing process and the adequacy of the technical infrastructure. The committee recognizes that these are not the only issues and topics of concern and debate in this area. Nevertheless, the committee considers that developing consensus on these key issues will be a major step forward and accelerate the appropriate use and licensing of digital I&C systems in nuclear power plants.

In Phase 2 of the study, the committee was charged to identify criteria for review and acceptance of digital instrumentation and control technology in both retrofitted reactors and new reactors of advanced design; to characterize and evaluate alternative approaches to the certification or licensing of this technology; and, where sufficient scientific basis exists, recommend guidelines on the basis of which the USNRC can regulate and certify (or license) digital instrumentation and control technology, including means for identifying and addressing new issues that may result from future development of this technology. Where insufficient scientific basis exists to make such recommendations, the committee was to suggest ways in which the USNRC could acquire the required information.

In carrying out its Phase 2 charge, the committee limited its work to those issues identified in Phase 1. Further, the reader should not form too literal an expectation that the committee has provided a cogent set of principles, design guidelines, and specific requirements for ready use by the USNRC to assess, test, license, and/or certify proposed systems and upgrades. Rather, the results of the committee's efforts are presented in the form of conclusions and recommendations related to each key issue and primarily addressed to the USNRC for their consideration and use for setting detailed licensing criteria and guidelines for digital I&C applications in nuclear power plants. The report discusses the difficult and complex nature of the key issues and directions for developing consensus on assessment of digital technology. The committee outlined criteria where it was possible to do so but focused primarily on (a) process both in developing guidelines and in the short-term acceptance of new technology; (b) identifying promising approaches for further actions by the USNRC beyond the committee's report; (c) suggestions for avoiding dead-ends; and (d) mechanics for improving communication and strengthening technical infrastructure at the USNRC. To carry out its work, the committee held a number of meetings, including site visits to several power plant facilities and simulators (see Appendix B). The committee also held detailed discussions with members of the staff of the U.S. Nuclear Regulatory Commission, the Nuclear Safety Research Review Committee, the Advisory Committee on Reactor Safeguards, members of the U.S. and foreign nuclear industries, and representatives from other safety-critical industries, who provided a variety of perspectives and information on digital instrumentation and control technology and its regulation. The committee is grateful to the many individuals who provided technical information and insights on this topic during briefings and site visits.

The chairman is also particularly grateful to the members of this committee who worked diligently and effectively on a very demanding schedule to meet a very difficult charge and produce this work. Special commendation and thanks are also extended to Tracy Wilson of the staff of the National Research Council, who was a pillar of strength and whose never failing energy and focus greatly facilitated the work of the committee.

Douglas M. Chapin
Committee Chair

Contents

APPENDICES

List of Tables and Figures

TABLES

FIGURES

Acronyms

ABB	Asea Brown Boveri
ABWR	advanced boiling water reactor
ACRS	Advisory Committee on Reactor Safeguards
ANS	American Nuclear Society
ANSI	American National Standards Institute
APWR	advanced pressurized water reactor
ASIC	application-specific integrated circuit
ATWS	anticipated transient without scram
BEES	Board on Energy and Environmental Systems
CETS	Commission on Engineering and Technical Systems
CFR	Code of Federal Regulations
CMF	common-mode failure
COTS	commercial off-the-shelf
EDF	Electricité de France
EMI	electromagnetic interference
EPRI	Electric Power Research Institute
EPS	emergency power system
ESFAS	engineered safety features actuation system
FPGA	field programmable gate arrays
FSAR	final safety analysis report
FTA	fault tree analysis
GE	General Electric
GL	generic letter
HCI	human-computer interface
HSI	human-system interface
I&C	instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute for Nuclear Power Operations
ISA	International Society for Measurement and Control
MTTF	mean time to failure
NEI	Nuclear Energy Institute
NRR	Office of Nuclear Reactor Regulation (USNRC)
NSRRC	Nuclear Safety Research Review Committee
NUSMG	Nuclear Utilities Software Management Group
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
RES	Office of Nuclear Regulatory Research (USNRC)
RFI	radiofrequency interference
RPS	reactor protection system
SAR	safety analysis report
SRP	Standard Review Plan
USNRC	U.S. Nuclear Regulatory Commission
USQ	unreviewed safety question

Digital Instrumentation and Control Systems in Nuclear Power Plants

Executive Summary

INTRODUCTION

Nuclear power plants rely on instrumentation and control (I&C) systems for monitoring, control, and protection. During their extensive service history, analog I&C systems have performed their intended monitoring and control functions satisfactorily. Although there have been some design problems, such as inaccurate design specifications and susceptibility to certain environmental conditions, the primary concern with the extended use of analog systems is effects of aging, e.g., mechanical failures, environmental degradation, and obsolescence.

The industrial base has largely moved to digital-based systems[1] and vendors are gradually discontinuing support and stocking of needed analog spare parts. The reason for the transition to digital I&C systems lies in their important advantages over existing analog systems. Digital electronics are essentially free of the drift that afflicts analog electronics, so they maintain their calibration better.[2] They have improved system performance in terms of accuracy and computational capabilities. They have higher data handling and storage capacities, so operating conditions can be more fully measured and displayed. Properly designed, they can be easier to use and more flexible in application. Indeed, digital systems have the potential for improved capabilities (e.g., fault tolerance, self-testing, signal validation, process system diagnostics) that could form the basis for entirely new approaches to achieve the required reliabilities. Because of such potential advantages, and because of the general shift to digital systems and waning vendor support for analog systems, the U.S. nuclear power industry expects substantial replacement of existing, aging analog systems with digital I&C technology. For the same reasons, designs for new, advanced nuclear power plants rely exclusively on digital I&C systems.

Challenges to Successful Introduction of Digital Instrumentation and Control Systems

Successful introduction of digital I&C systems into U.S. nuclear power plants faces several challenges:

- uncertainty inherent in introduction of new technology
- shift of existing technology base from analog experience
- technical problems identified from some applications of digital I&C in nuclear power plants
- difficult, time-consuming, and customized licensing approach
- lack of consensus (between the U.S. Nuclear Regulatory Commission [USNRC] and the regulated industry) on issues underlying evaluation and adoption of digital I&C technology and means to obtain a satisfactory resolution

In essence, the problem is to develop a systematic regulatory review and approval methodology for digital I&C systems that allows obtaining the safety and reliability benefits available from this technology while avoiding the introduction of offsetting safety problems.

The transition from analog to digital I&C systems in nuclear power plants is not straightforward; one must carefully account for the ways in which digital I&C implementations are different and frame regulations that reflect those differences.

Response of the U.S. Nuclear Regulatory Commission to the Challenges

The USNRC has reviewed a number of analog-to-digital "retrofits" in nuclear power plant I&C systems and is in the

[1] The committee intentionally avoided partitioning digital systems between hardware and software; rather the committee believes that digital systems are better treated in an integrated manner. Nevertheless, some of the specific topics addressed in the report merited discussion as "hardware" or "software" items.

[2] The reader should note, however, that since most sensors will remain analog-based, drift will not be eliminated, though it will likely be improved, especially if the digital I&C component contains software specifically designed to offset expected sensor drift.

process of reviewing designs of advanced plants. However, the review process has largely been customized for each application because of the lack of agreed-upon applicable criteria.[3] In addition, advisory committees, including the Advisory Committee on Reactor Safeguards (ACRS) and the Nuclear Safety Research Review Committee (NSRRC), have expressed concern that the USNRC may be lagging behind in its understanding of digital I&C systems and have urged the development of a framework to guide the regulation of digital I&C technology.

To address technical concerns, and in hopes of developing a wide consensus across the USNRC and the nuclear industry for a regulatory program, the USNRC held a workshop in September 1993. While a useful forum, the workshop did not lead to a consensus, and the USNRC requested the assistance of the National Research Council.

THIS STUDY

Committee's Task

The National Research Council was asked by the USNRC to conduct a study (including a workshop) on application of digital I&C technology to commercial nuclear power plant operations. The National Research Council accordingly appointed a committee (hereafter the committee) to carry out the study, which was conducted in two phases. In Phase 1, the committee was charged to define the important safety and reliability issues that arise from the introduction of digital I&C technology in nuclear power plant operations, including operations under steady-state, transient, and accident operating conditions. In response to this charge, the committee identified eight key issues associated with the use of digital I&C systems in existing and advanced nuclear power plants.

In Phase 2 of the study, the committee was charged to identify criteria for review and acceptance of digital I&C technology in both retrofitted reactors and new reactors of advanced design; to characterize and evaluate alternative approaches to the certification or licensing of this technology; and where sufficient scientific basis exists, recommend guidelines on the basis of which the USNRC can regulate and certify (or license) digital I&C technology, including means for identifying and addressing new issues that may result from future development of this technology. In areas lacking sufficient scientific basis to make such recommendations, the committee was to suggest ways in which the USNRC could acquire the required information.

In carrying out its Phase 2 charge, the committee limited its work to those issues identified in Phase 1. The issues were chosen because they were difficult and controversial. Further, the committee recognized that by law, the responsibility for setting licensing criteria and guidelines for digital I&C applications in nuclear plants rests with the USNRC. Thus, the reader should not form too literal an expectation that the committee has provided a cogent set of principles, design guidelines, and specific requirements for ready use by the USNRC to assess, test, license, and/or certify proposed systems or upgrades. Rather, the results of the study are presented in the form of conclusions and recommendations related to each issue and primarily addressed to the USNRC for their consideration and use. In the committee's view, there is substantial further work to be accomplished. The committee expects the USNRC and the nuclear industry to extend the work of criteria development beyond where this Phase 2 report leaves it. To guide further work, the committee's report offers findings and recommendations in four broad categories: (a) current practice that is essentially satisfactory or requires some fine tuning, (b) points of weakness in the USNRC's approach, (c) issues that merit further inquiry and research before satisfactory regulatory criteria can be developed, and (d) criteria and guidelines that are unreasonable to expect in the near future.

KEY ISSUES

Digital instrumentation and control systems for nuclear power plants have technological characteristics—equipment, response time, input and output range, and accuracy—very similar to those of digital instrumentation and control systems for other safety-critical applications such as chemical plants and aircraft. What distinguishes digital I&C applications in nuclear power plants from other digital I&C applications is the need to establish very high levels of reliability and safety under a wide range of conditions. Because of the potentially far greater consequences of accidents in nuclear power plants, the I&C systems must be relied upon to reduce the likelihood of even low-probability events. The USNRC has developed a regulatory process with the goal of achieving these high levels of reliability and thus assuring public safety. This process is subject to public scrutiny.

Developing the Key Issues (Phase 1)

In Phase 1 of the study, the committee identified eight key issues associated with the use of digital I&C systems in existing and advanced nuclear power plants. In the committee's view, these issues need to be addressed and a working consensus needs to be established regarding these issues among designers, operators and those responsible for

[3] Licensing of any systems for use in a nuclear power plant is governed by formal, documented criteria that the USNRC and the regulated industry use to implement changes to a nuclear power plant. General criteria, applicable to either digital or analog I&C systems in nuclear plants, are contained in the Code of Federal Regulations, Part 50, Appendix A. This very general guidance is supplemented by more specific guidance in various forms such as "regulatory guides" that endorse industry standards or interpret USNRC regulations. To date, the more specific regulatory criteria for digital I&C have largely been determined on a case-by-case basis rather than as generally applicable criteria.

maintenance of such systems, and regulators in the nuclear industry. The process the committee followed to identify these issues is discussed in the Phase 1 report and is only briefly summarized here.

In essence, the committee considered the impact of digital I&C systems against a set of standard regulatory approaches to assessing and ensuring safety (defense-in-depth, safety margins, environmental qualification, quality assurance, and failure invulnerability). From this analysis, the committee identified a number of questions and issues. After extensive deliberations, the committee selected eight key issues.

The eight issues can be separated into six technical issues and two strategic issues. The six technical issues are systems aspects of digital I&C technology, software quality assurance, common-mode software failure potential, safety and reliability assessment methods, human factors and human-machine interfaces, and dedication of commercial off-the-shelf hardware and software. The two strategic issues are the case-by-case licensing process and the adequacy of technical infrastructure (i.e., training, staffing, research plan). The committee recognizes that these are not the only issues and topics of concern and debate in this area. Nevertheless, the committee reaffirms its judgment, initially formed during Phase 1, that developing a consensus on these eight issues will be a major step forward and accelerate the appropriate use and licensing of digital I&C systems in nuclear power plants.

Analyzing the Key Issues (Phase 2)

In conducting Phase 2 of its study the committee employed a systematic process, which is reflected in the structure of most of the chapters in this report. The committee reviewed a large number of documents made available by the USNRC and variety of other sources. The committee also interviewed selected personnel from the USNRC, from the two advisory committees discussed above (ACRS, NSRRC), from the nuclear industry,[4] and from other industries[5] using digital systems in safety-critical applications. The committee also sought the view of individuals from academia and research organizations. In addition, the committee visited control room simulators, a nuclear plant, and a fossil-fueled power plant with extensive digital I&C systems. The committee also had frequent and detailed internal discussions, both face-to-face and via paper and electronic communications. The committee also brought to bear a wide range of experience in and knowledge of the field.

Carrying Out the Charge

The committee took seriously the charge that it identify criteria for review and acceptance of digital I&C technology and that it recommend guidelines for regulation and certification. In carrying out its charge, the committee recognized that:

- In order to develop useful guidance, only a limited number of issues could be dealt with in the relatively brief duration of the study.
- General, high level criteria would not be particularly useful.
- The final criteria are legally the USNRC's responsibility. Further, since the nuclear power industry is heavily regulated in the public interest, the licensing criteria should be forged in a detailed interaction among the regulators, the industry, and the public.
- The committee has a wide range of expertise and experience in digital systems and nuclear power plants but it is not a surrogate for this interaction among the stakeholders. Hence, the committee could serve by clearly delineating and defining issues and providing guidance for resolving these issues rather than developing specific licensing criteria.

Accordingly, the committee selected eight issues for study and worked on those issues. These eight issues address the two major intertwined themes associated with the use of digital instrumentation and control in nuclear power plants. These are:

1. Dealing with the specific characteristics of digital I&C technology as applied to nuclear power plants.
2. Dealing with a technology that is more advanced than the one widely in use in the existing nuclear power plants. This technology is rapidly advancing at a rate and in directions largely uncontrolled by the nuclear industry but at the same time likely to have a significant impact on the operation and regulation of the nuclear industry.

The technical issues the committee focuses on first in this report are primarily related to digital technology itself (Theme 1), while the strategic issues that follow are primarily related to the process of adopting advanced technology (Theme 2). The committee concentrated on reviewing the current approaches being taken by the nuclear industry and its regulators toward dealing with the selected key issues. The committee also tried to learn from the experience of the international nuclear industry as well as gather and evaluate information about how other safety-critical industries and their regulators dealt with these issues. Also, through the technical expertise and knowledge of its various members, the committee explored work done by the digital systems community at large, including both research activities and academic work.

[4] These individuals were from the U.S. domestic industry and also from Japan, Canada, and the United Kingdom. The committee also reviewed literature on the French nuclear program.

[5] These individuals were from the railroad, aerospace, defense, and medical products industry.

As the committee worked through the issues it discovered there is a major impediment to progress. This is the communication barriers that exist among the key technical communities and individuals involved. The basic reason for the communication difficulty is apparent. Work is simultaneously going on in many areas, each with its own technology, research focus, and agenda. Unfortunately, although many of these areas use common terms, these terms often have different meanings to different groups, resulting in either a lack of communication or very difficult communication. This is particularly troublesome for the nuclear power industry and its regulators, who are not dominant in this technology and must try to synthesize information and experience from a variety of sources and apply it in power plants where safety hazards must be dealt with in a rigorous way, under public scrutiny. In Chapter 11 the committee discusses this communication problem in more detail and provides suggestions for a way forward. Making substantial progress in this area should have a multiplicative effect as it eases the resolution of many specific technical and strategic issues.

Overall, while there are important steps that remain to be taken by the USNRC and industry as addressed in this report, the committee found no insurmountable barriers to the use of digital instrumentation and control technology to nuclear power plants. The committee also believes that a forward-looking regulatory process with good and continuing regulations and industry communication and interaction will help. All participants must recognize that crisp, hard-edged criteria are particularly difficult to come by in this rapidly moving area and good practices and engineering judgment will continue to be needed and relied upon.

For the key technical issues (systems aspects of digital I&C technology; software quality assurance; common-mode software failure potential; safety and reliability assessment methods; human factors and human-machine interfaces; and dedication of commercial off-the-shelf hardware and software) the committee provides specific recommendations and conclusions which include a number of specific criteria. These are listed in each chapter (see Chapters 3 through 8). But recognizing the difficulty of defining specific criteria, and the need for the nuclear technology stakeholders, particularly the USNRC, to make the final decisions, the committee focused on (a) providing process guidance both in developing guidelines and in the short-term acceptance of the new technology; (b) identifying promising approaches to developing criteria and suggestions for avoiding dead-ends; and (c) mechanics for improving communication and strengthening technical infrastructure.

For the key strategic issues (the case-by-case licensing procedure and adequacy of the technical infrastructure) the committee:

- Emphasizes guidance to implement a generically applicable framework for regulation that follows current USNRC practice and draws a distinction between major and minor safety modifications. The committee also provides guidance for the evaluation and updating of this regulatory framework (see Chapter 9).
- Identifies a need to upgrade the current USNRC technical infrastructure and suggests specific research activities that will support the needed regulatory program and USNRC's research needs. The committee also suggests several improvements to the technical infrastructure to improve and maintain technical capabilities in this rapidly moving, technically challenging area.

The results of this process are set forth below, where the committee introduces each of the key issues—first the technical, then the strategic—with an "issue statement" developed during Phase 1 of the study. Following each issue statement are the conclusions and recommendations formulated by the committee during Phase 2 of the study.

TECHNICAL ISSUES

Systems Aspects of Digital Instrumentation and Control Technology

Issue Statement. Along with important benefits, digital I&C systems introduce potential new failure modes that can affect operations and margins of safety. Therefore, digital I&C systems require rigorous treatment of the systems aspects of their design and implementation. What methods are needed to address this concern? How can the experience and best practices of the various technical communities involved in applying digital I&C technologies be best integrated and applied to nuclear power plants? What procedures can be put in place to update the methods and the experience base as new digital I&C technologies and equipment are introduced in the future?

Conclusion 1. Continued effort is warranted by the USNRC and the nuclear industry to deal with the systems aspects of digital I&C in nuclear power plants.

Conclusion 2. The lack of actual design and implementation of large I&C systems for U.S. nuclear power plants makes it difficult to use learning from experience as a basis for improving how the nuclear industry and the USNRC deal with systems aspects.

Conclusion 3. The USNRC's intent to upgrade their regulatory guidance in the systems aspects of digital I&C applications in nuclear power plants is entirely supported by the committee's observations about systems aspects.

Conclusion 4. Existing regulatory guidance lacks the specificity needed to be effective, and the revision should address this shortcoming.

Recommendation 1. The USNRC should make a trial application of the proposed regulatory guidance documents on systems aspects to foreign nuclear plant digital systems, both existing and in progress. In particular, this review should focus on assessing whether or not the revised guidance documents have the necessary level of specificity to adequately address the systems aspects of nuclear plant digital I&C implementations.

Recommendation 2. The USNRC should identify and review systems aspects guidance documents provided in other industries, such as chemical processing and aerospace, where large-scale digital I&C systems are used. The focus of this review would be to compare these other guidance documents with those being developed by the USNRC, paying due attention to common problems and application-specific differences.

Recommendation 3. To obtain practical experience, the USNRC should loan staff personnel, perhaps on a reciprocal basis, to other agencies involved in regulating or overseeing large safety-critical digital I&C systems.

Recommendation 4. The USNRC should require continuing professional training for appropriate staff in technologies particularly germane to systems aspects, such as fault-tolerant, distributed systems.

Software Quality Assurance

Issue Statement. The use of software is a principal difference between digital and analog I&C systems. Quality of software is measured in terms of its ability to perform its intended functions. This, in turn, is traced to software specifications and compliance with these specifications. Neither of the classic approaches of (a) controlling the software development process or (b) verifying the end-product appears to be fully satisfactory in assuring adequate quality of software, particularly for use with safety-critical systems. How can the USNRC and the nuclear industry define a generally accepted, technically sound solution to specifying, producing, and controlling software needed in digital I&C systems?

Conclusion 1. Software quality assurance procedures typically monitor process compliance rather than product quality. In particular, there are no generally accepted evaluation criteria for safety-related software; rather, standards and guidelines help to repeat best practices. Because most software qualities related to system safety, e.g., maintainability, correctness, and security, cannot be measured directly, it must be assumed that a relationship exists between measurable variables and the qualities to be ensured. To deal with this limitation, care must be taken to validate such models, e.g., using past development activities, and to assure that the measurements being made are appropriate and accurate in assessing the desired software qualities.

Conclusion 2. Prior operating experience with particular software does not necessarily ensure reliability or safety properties in a new application. Additional reviews, analysis, or testing by a utility or third-party dedicator may be necessary to reach an adequate level of assurance.

Conclusion 3. Testing must not be the sole quality assurance technique. In general, it is not feasible to assure software correctness through exhaustive testing for most real, practical I&C systems.

Conclusion 4. USNRC staff reviews of the verification and validation process used during software development seem quite thorough.

Conclusion 5. Exposing software flaws, demonstrating reliable behavior of software, and finding unintended functionality and flaws in requirements are different concepts and should be assessed by a combination of techniques including:

- Systematic inspections of software and planned testing with representative inputs from different parts of the systems domain can help determine if flaws exist in the software.
- Functional tests can be chosen to expose errors in normal and boundary cases, and measures of test coverage can be reported for them.
- Testing based on large numbers of inputs randomly selected from the operational profiles of a program can be used to assess the likelihood that software will fail under specific operating conditions.
- Requirements inspections can be an effective method for detecting software defects, provided requirements are studied by several experienced people who did not participate in their construction. The effectiveness of these reviews also depends on the quality of the requirements.
- A system-level hazard analysis can identify states that, combined with environmental conditions, can lead to accidents. The analysis should extend into software components to ensure that software does not contribute to system hazards.

Conclusion 6. The USNRC research programs related to software quality assurance appear to be skewed toward investigating code-level issues, e.g., coding in different languages to achieve diversity and program slicing to identify threads containing common code.

Conclusion 7. Rigorous configuration management must be used to assure that changes are correctly designed and implemented and that relationships between different software artifacts are maintained.

Conclusion 8. Software is not more testable simply because the design has been implemented on a chip. Use of any technology requiring equivalent design effort to software requires commensurate quality assurance. For example, this conclusion applies to ASIC (application-specific integrated circuit), PLC (programmable logic controllers), and FPGA (field programmable gate arrays). However, the committee notes that these technologies may be useful in addressing some configuration management problems.

Recommendation 1. Currently, the USNRC's path is to develop regulatory guides to endorse (with possible exceptions) a variety of industry standards. The USNRC should develop its own guidelines for software quality assurance that focus on acceptance criteria rather than prescriptive solutions. The draft regulatory guide, Software in Protection and Control Systems, by Canada's Atomic Energy Control Board is an example of this type of approach. The USNRC guidelines should be subjected to a broad-based, external peer review process including (a) the nuclear industry, (b) other safety-critical industries, and (c) both the commercial and academic software communities.

Recommendation 2. Systems requirements should be written in a language with a precise meaning so that general properties like consistency and completeness, as well as application-specific properties, can be analyzed. Cognizant personnel such as plant engineers, regulators, system architects, and software developers should be able to understand the language.

Recommendation 3. USNRC research in the software quality assurance area should be balanced in emphasis between early phases of the software life cycle and code-level issues. Experience shows that the early phases contribute more frequently to the generation of software errors.

Recommendation 4. The USNRC should require a commensurate quality assurance process for ASICs, PLCs, and other similar technologies.

Common-Mode Software Failure Potential

Issue Statement. Digital technology introduces a possibility that common-mode software failures may cause redundant safety systems to fail in such a way that there is a loss of safety function. Various procedures have been developed and evolved for evaluating common-mode failure potential in analog devices. Do these same procedures apply to computers and software or are different approaches to ensuring reliability needed? What does software diversity mean? Can it be achieved and assessed and, if so, how? Do techniques exist for assessing common-cause failure and common-mode failure when computers are involved? What are the implications of common-mode software failure for the licensing process and the use of component diversity? Are redundancy and diversity the most effective way to achieve reliability for digital systems?

Conclusion 1. The USNRC position of assuming that common-mode software failure could occur is credible, conforms to engineering practice, and should be retained.

Conclusion 2. The USNRC position with respect to diversity, as stated in the draft branch technical position, Digital Instrumentation and Control Systems in Advanced Plants, and its counterpart for existing plants, is appropriate.

Conclusion 3. The USNRC guidelines on assessing whether adequate diversity exists need to be reconsidered. With regard to these guidelines: (a) The committee agrees that providing digital systems (components) that perform different functions is a potentially effective means of achieving diversity. Analysis of software functional diversity showing that independence is maintained at the system level and no new failure modes have been introduced by the use of digital technology is no different from that for upgrades or designs that include analog instrumentation. (b) The committee considers that the use of different hardware or real-time operating systems is potentially effective in achieving diversity provided functional diversity has been demonstrated. With regard to real-time operating systems, this applies only to operating systems developed by different companies or shown to be functionally diverse. (c) The committee does not agree that use of different programming languages, different design approaches meeting the same functional requirements, different design teams, or different vendors' equipment used to perform the same function is likely to be effective in achieving diversity. That is, none of these methods is a proof of independence of failures. Conversely, neither is the presence of these proof of dependence of failures.

Conclusion 4. There appears to be no generally applicable, effective way to evaluate diversity between two pieces of software performing the same function. Superficial or surface (syntactic) differences do not imply failure independence, nor does the use of different algorithms to achieve the same functions. Therefore, funding research to try to evaluate design diversity does not appear to be a reasonable use of USNRC research funds.

Conclusion 5. Although many in the software community believe that there are more cost-effective techniques for achieving high software reliability than redundancy and diversity, there is no agreement as to what these alternatives may be. The most promising of these appear to be the extension of standard safety analysis and design techniques to software and the use of formal (mathematical) analysis.

Conclusion 6. The use of self-checking to detect hardware failures and some simple software errors is effective and should be incorporated. However, care must be taken to assure that the self-checking features themselves do not introduce errors.

Recommendation 1. The USNRC should retain its position of assuming that common-mode software failure is credible.

Recommendation 2. The USNRC should maintain its basic position regarding the need for diversity in digital I&C systems as stated in the draft branch technical position, Digital

Instrumentation and Control Systems in Advanced Plants (see Chapter 5), and its counterpart for existing plants.

Recommendation 3. The USNRC should revisit its guidelines on assessing whether adequate diversity exists. The USNRC should not place reliance on different programming languages, different design approaches meeting the same functional requirements, different design teams, or using different vendors' equipment ("nameplate" diversity). Rather, the USNRC should emphasize potentially more robust techniques such as the use of functional diversity, different hardware, and different real-time operating systems.

Recommendation 4. The USNRC should reconsider the use of research funding to try to establish diversity between two pieces of software performing the same function. This does not appear to be possible. Specifically, it appears the USNRC funding of the Unravel tool is based on the use of this tool for this purpose and, as such, is unlikely to be useful.

Safety and Reliability Assessment Methods

Issue Statement. Effective, efficient methods are needed to assess the safety and reliability of digital I&C systems in nuclear power plants. These methods are needed to help avoid potentially unsafe or unreliable applications and aid in identifying and accepting safety-enhancing and reliability-enhancing applications. What methods should be used for making these safety and reliability assessments of digital I&C systems?

Conclusion 1. Deterministic assessment methodologies, including design basis accident analysis, hazard analysis, and other formal analysis procedures, are applicable to digital systems.

Conclusion 2. There is controversy within the software engineering community as to whether an accurate failure probability can be assessed for software or even whether software fails randomly (see Chapter 6). However, the committee agreed that a software failure probability can be used for the purposes of performing probabilistic risk assessment (PRA) in order to determine the relative influence of digital system failure on the overall system. Explicitly including software failures in a PRA for a nuclear power plant is preferable to the alternative of ignoring software failures.

Conclusion 3. The assignment of probabilities of failure for software (and more generally for digital systems) is not substantially different from the handling of many of the probabilities for rare events. A good software quality assurance methodology is a prerequisite to providing a basis for the generation of bounded estimates for software failure probability. Within the PRA, uncertainty and sensitivity analysis can help the analyst assure that the results are not unduly dependent on parameters that are uncertain. As in other PRA computations, bounded estimates for software failure probabilities can be obtained by processes that include valid random testing and expert judgment.[6]

Conclusion 4. Probabilistic analysis is theoretically applicable in the same manner to commercial off-the-shelf (COTS) equipment, but the practical application may be difficult. The difficulty arises when attempting to use field experience to assess a failure probability, in that the experience may or may not be equivalent. For programmable devices, the software failure probability may be unique for each application. However, a set of rigorous tests may still be applicable to bounding the failure probability, as with custom systems. A long history of successful field experience may be useful in eliciting expert judgment.

Recommendation 1. The USNRC should require that the relative influence of software failure on system reliability be included in PRAs for systems that include digital components.

Recommendation 2. The USNRC should strive to develop methods for estimating the failure probabilities of digital systems, including COTS, for use in probabilistic risk assessment. These methods should include acceptance criteria, guidelines and limitations for use, and any needed rationale and justification.

Recommendation 3. The USNRC and industry should evaluate their capabilities and develop a sufficient level of expertise to understand the requirements for gaining confidence in digital implementations of system functions and the limitations of quantitative assessment.

Recommendation 4. The USNRC should consider support of programs that are aimed at developing advanced techniques for analysis of digital systems that might be used to increase confidence and reduce uncertainty in quantitative assessments.

Human Factors and Human-Machine Interfaces

Issue Statement. At this time, there does not seem to be an agreed-upon, effective methodology for designers, owner-operators, maintainers, and regulators to assess the overall impact of computer-based, human-machine interfaces on human performance in nuclear power plants. What methodology and approach should be used to assure proper consideration of human factors and human-machine interfaces?

Conclusion 1. Digital technology offers the potential to enhance the human-machine interface and thus overall operator performance. Human factors and human-machine interfaces are well enough understood that they do not represent a major barrier to the use of digital I&C systems in nuclear power plants.

[6] Committee member Nancy Leveson did not concur with this conclusion.

Conclusion 2. The methodology and approach adopted by the USNRC for reviewing human factors and human-machine interfaces provides an initial and acceptable first step in a review. Existing USNRC procedures, for both the design product and process, are consistent with those of other industries. The guidelines are based on many already available in the literature or developed by specific industries. The methodology for reviewing the design process is based on sound system engineering principles consistent with the validation and verification of effective human factors.

Conclusion 3. Adequate design must go beyond guidelines. The discussion in NUREG-0711 on advanced technology and human performance and the design principles set out in Appendix A of NUREG-0700 Rev. 1 provide a framework within which the nuclear industry can specify, prototype, and empirically evaluate a proposed design. Demonstration that a design adheres to general principles of good human-system integration and takes into account known characteristics of human performance provides a viable framework in which implementation of somewhat intangible, but important, concepts can be assessed.

Conclusion 4. There is a wide range in the type and magnitude of the digital upgrades that can be made to safety and safety-related systems. It is important for the magnitude of the human factors review and evaluation to be commensurate with the magnitude of the change. Any change, however, that affects what information the operator sees or the system's response to a control input must be empirically evaluated to ensure that the new design does not compromise human-system interaction effectiveness.

Conclusion 5. The USNRC is not sufficiently active in the public human factors forum. For example, proposed human factors procedures and policies or sponsored research, such as NUREG-0700 Rev. 1, are not regularly presented and reviewed by the more general national and international human factors communities, including such organizations as the U.S. Human Factors and Ergonomics Society, Institute of Electrical and Electronics Engineers (IEEE), Society on Systems, Man, and Cybernetics, and the Association of Computing Machinery Special Interest Group on Computer-Human Interaction. European nuclear human factors researchers have used nuclear power plant human factors research to further a better understanding of human performance issues in both nuclear power plants and other safety-critical industries. Other safety-critical U.S. industries, such as space, aviation, and defense, participate actively, benefiting from the review and experience of others.

Recommendation 1. The USNRC should continue to use, where appropriate, review guidelines for both the design product and process. Care should be taken to update these guidelines as knowledge and conventional wisdom evolve—in both nuclear and nonnuclear applications.

Recommendation 2. The USNRC should assure that its reviews are not limited to guidelines or checklists. Designs should be assessed with respect to (a) the operator models that underlie the them, (b) ways in which the designs address classic human-system interaction design problems, and (c) performance-based evaluations. Moreover, evaluations must use representative tasks, actual system dynamics, and real operators.

Recommendation 3. The USNRC should expand its review criteria to include a catalog or listing of classic human-machine interaction deficiencies that recur in many safety-critical applications. Understanding the problems and proposed solutions in other industries is a cost-effective way to avoid repeating the mistakes of others as digital technology is introduced into safety and safety-related nuclear systems.

Recommendation 4. Complementing Recommendation 2, although human factors reviews should be undertaken seriously, e.g., in a performance-based manner with realistic conditions and operators, the magnitude and range of the review should be commensurate with the nature and magnitude of the digital change.

Recommendation 5. The USNRC and the nuclear industry at large should regularly participate in the public forum. As noted in NUREG-0711, advanced human interface technologies potentially introduce many new, and as yet unresolved, human factors issues. It is crucial that the USNRC stay abreast of current research and best practices in other industries, and contribute findings from its own applications to the research and practitioner communities at large—for both review and education. (See also Technical Infrastructure chapter for additional discussion.)

Recommendation 6. The USNRC should encourage researchers with the Halden Reactor Project to actively participate in the international research forum to both share their results and learn from the efforts of others.

Recommendation 7. As funds are available, the USNRC's Office of Nuclear Regulatory Research should support research exploring higher-level issues of human-system integration, control, and automation. Such research should include exploration, specifically for nuclear power plant applications, of design methods, such as operator models, for more effectively specifying a design. Moreover, extensive field studies should be conducted to identify nuclear-specific technology problems and to compare and contrast the experiences in nuclear application with those of other safety-critical industries. Such research will add to the catalog of recurring deficiencies and potentially link them to proposed solutions.

Recommendation 8. Complementing its own research projects, the USNRC should consider coordinating a facility, perhaps with the U.S. Department of Energy, in which U.S. nuclear industries can prototype and empirically evaluate proposed designs. Inexpensive workstation technologies permit the development of high-fidelity workstation-based simulators of significant portions of control rooms. Other industries make extensive use of workstation-based part-task simulators (e.g., aviation); results are found to scale quite well to the systems as a whole.

Dedication of Commercial Off-the-Shelf Hardware and Software

Issue Statement. What methods should be agreed upon by the regulators and the licensees to evaluate and accept the use of commercial off-the-shelf digital I&C systems in safety applications in nuclear power plants?

Conclusion 1. Use of COTS hardware and software is an attractive possibility for the nuclear industry to pursue, provided that a technically adequate dedication process can be formulated and that this process does not negate the cost advantages of COTS.

Conclusion 2. The recently developed draft guideline of the Electric Power Research Institute (EPRI) working group, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, appears to have potential as the basis for reaching industry and USNRC consensus on the COTS issue. In view of this possibility, the committee notes that the guideline and the follow-on (second-tier) guidance should assure that the necessary and sufficient attributes of digital I&C application are defined for both hardware and software. Once these attributes are well-defined, various acceptable methods of assessing the validity of the attributes can be more readily ascertained and used and the requisite experience gained. As an example of the type of approach the committee considers appropriate, the EPRI working group and the USNRC staff should consider the FAA's DO-178B guideline for digital avionics, Software Considerations in Airborne Systems and Equipment Certification, which includes guidance on COTS.

Conclusion 3. Software quality assurance and safety and reliability assessment methods are strongly related to COTS. The committee's conclusions in Chapters 4 and 6, respectively, should therefore also be considered. Dedication processes for COTS should also prove relevant in cases where standardized software is reused among similar nuclear applications.

Conclusion 4. The USNRC involvement in the EPRI, Nuclear Utilities Software Management Group (NUSMG), IEEE, and International Society for Measurement and Control (ISA) working groups is very useful and should aid the USNRC in developing specific guidance to address the COTS issue.

Conclusion 5. The approach to COTS must apply criteria and verification activities commensurate with the safety significance and complexity of a specific application. For example, the level of verification activities applied to small-scale replacements of recorders and indicators would not be the same as that applied to large-scale replacements of reactor protection systems.

Recommendation 1. The USNRC staff should assure that their involvement in the EPRI, NUSMG, IEEE, and ISA working groups means that USNRC concerns and positions are being addressed so that any standards or guidelines developed by these groups can be quickly accepted and endorsed by the USNRC.

Recommendation 2. The USNRC should establish what research is needed to support USNRC acceptance of COTS in safety applications in nuclear plants. This research should then be incorporated into the overall research plan.

Recommendation 3. The USNRC regulatory guidance on the use of COTS should recognize and be based on the principle that criteria and verification activities are to be commensurate with the safety significance and complexity of the specific application.

STRATEGIC ISSUES

Case-by-Case Licensing Process

Issue Statement. What changes should be considered in the regulatory process to provide more efficient and effective regulation of digital I&C systems in nuclear power plants? How can sufficient flexibility be incorporated to address the rapidly changing nature of the digital I&C technology and better match the time response of the regulatory process to the technology it controls? How can the regulatory process be made more efficient while maintaining its technical integrity?

Conclusion 1. As a general observation, the role of the regulator in overseeing the implementation of digital upgrades can be a valuable and important one. Particularly in an area such as digital I&C systems, where the state of the art evolves rapidly and where first-of-a-kind nuclear applications are contemplated, the oversight role of the regulator can bring valuable insights to the implementation of such upgrades. Indeed, the committee found several specific examples of this happening.

Conclusion 2. Nevertheless, the committee found that the regulatory response to the development and implementation of digital I&C upgrades in nuclear plants has proceeded in a manner that resulted in some degree of confusion and uncertainty within the licensee community with regard to the applicable regulatory requirements and the procedural framework for implementing such upgrades. This uncertainty and the resultant incremental cost has been a major contributor to the reluctance on the part of utilities in proceeding with digital upgrades.

Conclusion 3. The lack of generically applicable regulatory requirements for digital upgrades has resulted in a case-by-case approach that has contributed to the confusion and uncertainty. This approach to reviews may have been necessary in the early phase of the transition to digital systems.

But the USNRC now has a sufficient body of experience with safety-related digital upgrades, gained over recent years and supplemented by the extensive experience of other countries and other industries, to enable the agency to establish a generically applicable regulatory regime that would govern the review and approval of such upgrades.

Conclusion 4. The process established in 10 CFR 50.59, wherein the agency has defined those circumstances where a licensee may make a modification without prior USNRC review and approval, is fundamentally sound, necessary, and consistent with the USNRC's responsibility to protect the public health and safety. In particular, it recognizes the practical necessity for licensees to make facility modifications consistent with their facility licensing basis, without the need for prior USNRC review and approval. Moreover, the process appropriately reflects the gradation of significance in changes that might be made in a nuclear plant and the USNRC's attendant role based upon these gradations. In this regard, the committee strongly believes that it is important for the USNRC to distinguish between digital upgrades that are significant (i.e., pose unreviewed safety questions) and those that are not, and tailor the scope and depth of the regulatory review in a manner that is commensurate with this gradation.

Conclusion 5. The committee believes that defining *all* safety-related digital upgrades as resulting in an unreviewed safety question, as stated in the USNRC's draft generic letter of August 1992, is contrary to both the letter and spirit of 10 CFR 50.59.

Conclusion 6. The agency has no formal process for cataloguing determinations made under 10 CFR 50.59 with regard to digital upgrades and the bases for these determinations. Such information would assist both the USNRC and the utilities in determining whether particular upgrades pose unreviewed safety questions.

Conclusion 7. Early interaction between a utility applicant and the USNRC can be extremely helpful in identifying and fleshing out important issues. Where this proactive interaction has occurred, the committee found that the subsequent regulatory review was more efficient and focused, minimizing resources that would otherwise be required on the part of both the utility and the USNRC.

Recommendation 1. The USNRC should place a high priority on its effort to develop a generically applicable framework for the review and evaluation of digital I&C upgrades for operating reactors.

Recommendation 2. In view of the rapid evolution of digital technology, a process should be established to ensure that the regulatory framework is updated to stay abreast of new developments. To ensure that this framework takes into account the best practices in other safety-critical industries, external and public review is highly desirable.

Recommendation 3. The USNRC should consider additional ways in which the guideline development process can be accelerated and streamlined. For example, consideration could be given to establishing chartered task groups involving representatives from the USNRC, the industry, and academia. These groups would be tasked and managed on a project basis to investigate and resolve unreviewed matters of possible safety significance that arise in the development and use of digital systems.

Recommendation 4. In developing its regulatory requirements, the USNRC should ensure that where issues arise that are unique to digital systems, they are treated appropriately. On the other hand, where issues arise with regard to digital upgrades that are no different from issues posed for analog systems, such issues should be treated consistently. The opportunity (or obligation) for the USNRC to review and approve digital upgrades should not be seen as an opportunity to impose new requirements on individual licensees unless the issue is unique to the application proposed.

Recommendation 5. In view of the substantial benefits of early interaction with individual utilities considering digital upgrades, as well as the benefit of working closely with industry groups and other interested members of the public in the development of standards and guidelines, the USNRC should undertake proactive efforts to interact early and frequently with individual utilities and with industry groups and other interested members of the public. In addition, it would be of benefit for the USNRC to be familiar with the broader evolving applications of digital I&C systems in both nuclear and nonnuclear applications. This, in turn, will provide a foundation for a cooperative working relationship.

Recommendation 6. The USNRC should revisit the "systems level" issue addressed in Generic Letter 95-02 and EPRI Report TR-102348 to ensure that this position is consistent with the historical interpretation of 10 CFR 50.59. The committee strongly endorses maintaining and formalizing the distinction between major and minor safety system upgrades containing digital technology.

Recommendation 7. The USNRC should establish a process for cataloguing 50.59 evaluations of digital upgrades in some centralized fashion, so that individual utilities considering such upgrades can review and consider past 50.59 determinations regarding when a particular modification has been found to result in an unreviewed safety question.

Adequacy of Technical Infrastructure

Issue Statement. Does the USNRC need to make changes in its staffing, training, and research program to support its regulation of digital I&C technology in nuclear power plants? If so, what is the appropriate program for the USNRC? How should this program be structured so that it maintains its effectiveness in the face of rapidly moving and developing technology and generally declining budgets?

Conclusion 1. The USNRC should make changes in its staffing, training, and research program to support its regulation of digital I&C technology in nuclear power plants. Specific recommendations are provided below.

Conclusion 2. The issue of adequate technical infrastructure is applicable not only to the USNRC but also to the nuclear industry as a whole. Many of the committee's recommendations for the USNRC have parallel applications to the nuclear industry.

Conclusion 3. The USNRC must anticipate that the regulatory technical infrastructure will continue to be challenged by advancing digital I&C technology. The focus of the near-term licensing effort will be on digital upgrades and certification of the advanced plants. The USNRC will have to continue to expand its technical infrastructure as use of digital technology expands and its sophistication increases.

Conclusion 4. There are problems inherent in the historical process for developing standards and industry guidelines, particularly those applied to the rapidly advancing digital technology. Pending development of alternate approaches, early involvement by the USNRC in developing standards and industry guidelines will foster more timely availability of regulatory guidance and acceptance criteria.

Conclusion 5. A strategic plan is needed for the USNRC research program on digital I&C applications. The current research program is a disjointed collection of studies lacking an underlying strategy and in some specific cases pursuing topics of questionable worth. The staff structure of the USNRC, which separates the staff of the Office of Nuclear Reactor Regulation (NRR) from the staff of the Office of Nuclear Regulatory Research (RES) and mandates that the RES staff respond to NRR "user needs," may be an obstacle to development of a coherent plan that balances near-term regulatory decision making and long-term research into problems on the horizon. Periodic outside review of the USNRC research program could help assure that the right issues are being addressed and could also lead to areas of collaborative research. The committee is aware of and notes favorably the impact of the existing Nuclear Safety Research Review Committee. However, a more formal, outside review would be useful. Perhaps this could be done on an exchange basis with other agencies to reduce resource demands.

Recommendation 1. Despite difficulties posed by declining budget and staffing levels in the face of rapidly moving technology and a stagnating nuclear industry, the USNRC must explore ways to improve the efficiency of the review process with existing staff and resources.

Recommendation 2. The USNRC should define a set of minimal and continuing training needs for existing and recruited staff. Particular attention should be paid to software quality assurance expertise. Once defined, the USNRC training program should be subjected to appropriate external review. Certification of USNRC expertise levels is one possibility the USNRC may wish to consider.

Recommendation 3. Consistent with Conclusion 5 above, the USNRC should develop a strategic plan for the research program conducted by the RES and NRR offices. The plan should emphasize balancing short-term regulatory needs and long-term, anticipatory research needs and should incorporate means of leveraging available resources to accomplish both sets of research objectives. It should also reach out more effectively to relevant technical communities (e.g., by the establishment of research simulators for human factors research), to the Electric Power Research Institute, to the Department of Energy, to foreign nuclear organizations, and to other safety-critical industries dealing with digital I&C issues. In making this recommendation, the committee recognizes the Halden Reactor Project provides an example of such cooperative research; but much of the Halden work cannot be published widely and therefore lacks the benefit of rigorous peer scrutiny.

Recommendation 4. Because research in the digital I&C area may require a longer time frame than that of single fiscal years, the USNRC should give consideration to planning and arranging funding on a multiyear basis.

Recommendation 5. Consistent with Conclusion 4 above, the USNRC should consider ways to accelerate preparation and updating of needed standards and guidance documents. In particular, the USNRC should consider using chartered task groups (see Recommendation 3 pertaining to the case-by-case licensing process).

CONCLUDING STATEMENT

The committee has presented what it believes to be a pragmatic approach for meeting the challenge. One key obstacle is overcoming impediments to communication.

There are a number of ways to address the communication difficulty. Some are already being pursued, some need to be initiated. The committee particularly emphasizes five areas of need:

- the need for better, clearer, crisper statements of the regulatory concern and the appropriate acceptance criteria that are valid at any point in time
- the need for the nuclear power industry and the USNRC to be more proactive in the relevant technical communities
- the need for the nuclear power industry and its regulator to strengthen its technical infrastructure in digital systems
- the need to formally address the communication problem in a systematic way

- the need to tune up the regulatory mechanisms that are employed when an advanced technology, like digital I&C, has temporarily outpaced the regulations

Turning to high-level issues more specifically related to digital technology, the committee emphasizes the following:

- The use of digital I&C technology does not obviate the standard methods for safety assessments of nuclear power plants.
- Digital I&C systems (and digital systems in general) should not be addressed only in terms of hardware or software.
- Most practical digital I&C systems cannot be exhaustively tested and therefore cannot be shown to be free from any and all errors.

In summary, the committee notes that digital instrumentation and control is state-of-the-art technology and is widely used both inside and outside the nuclear industry. Digital I&C systems offer powerful capabilities that can, however, affect nuclear power plant safety; therefore, digital systems should be treated carefully, particularly in safety-critical applications. It appears the USNRC and the nuclear power industry are moving forward with procedures, processes, and technical infrastructure needed to assure continued safe operation of the plants. The committee has suggested several improvements.

1

Introduction

NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL SYSTEMS

Role of Instrumentation and Control in Nuclear Power Plants

Nuclear power plants rely on instrumentation and control (I&C) systems for monitoring, control, and protection. The grouping of I&C systems according to these three types of functions (monitoring, control, and protection) is discussed in some detail below. There is, however, another division of I&C systems into two categories called within the nuclear industry "nonsafety" and "safety." The nonsafety systems are used by the operators to monitor and control the normal operation of the plant, including startup and shutdown, and to mitigate and prevent plant operational transients. These nonsafety systems are backed up by a set of independent (noninteracting), redundant safety systems that are designed to take automatic action to prevent and mitigate accident conditions if the operators and the nonsafety systems fail to maintain the plant within normal operating conditions. Thus to some extent (but not entirely) nonsafety systems coincide with monitoring and control systems, safety systems with protection systems. This is discussed further below.

The two categories of systems, safety and nonsafety, are thought of as being consistent with and part of the defense-in-depth approach to safety.[1] The distinction between them is important since essentially only the safety systems are "credited" (i.e., relied upon by the utility and the U.S. Nuclear Regulatory Commission [USNRC] as a basis for making judgments about safety) in the formal safety analyses of the plant. The safety systems are thus of particular concern in the USNRC's licensing procedures, whereas very few of the nonsafety systems fall under the same rigorous regulatory control. Before proceeding to further discussion of safety systems, however, it is in order to describe the three types of I&C systems in nuclear power plants.

Types of Instrumentation and Control Systems

In a nuclear power plant, the I&C systems—irrespective of whether they are analog or digital technology—are generally grouped into three types: plant monitoring and display systems, plant control systems, and plant protection and mitigation systems.

Plant Monitoring and Display Systems

Plant monitoring and display systems monitor plant variables and provide data to other I&C systems and to the plant operators for use in controlling the operation of the plant. Typical examples include systems that monitor and display the status of the fire protection system, fluid temperatures, and pressures. These systems also normally provide visual and audible alarms at various control stations, particularly the main control room, that notify operators of trends or particular values requiring action by the operator to avert an actual problem or emergency. Usually there are formal procedures the operators follow when such an alarm or notification occurs, with the alarm setpoint and required response time coordinated to give the operator adequate time to take action. Typically, the response times are on the order of tens of minutes; if inadequate time exists, an automated response is provided.

Plant Control Systems

Plant control systems are used to control all the normal operations of the plant. They are used in startup, power operations, shutdowns, and plant upsets. Regarded by plant owners as the primary controls for their expensive and complex plants, they are fully engineered, they are robust, and they usually have considerable redundancy (see below) to

[1] Defense-in-depth is the conservative design approach that uses multiple, layered systems to provide alternate means of accomplishing different functions related to common goals. This approach provides added protection against natural phenomena and plant operational transients.

prevent single failures or anticipated events from escalating into plant shutdowns, trips, or accidents endangering plant equipment, personnel, and the public. Typical examples include feedwater and steam control systems, turbine generator controls, and the myriad of systems used to control the many circuit breakers, pumps, and valves throughout the plant.

Plant Protection and Mitigation Systems

Plant protection and mitigation systems are an additional, separate layer of systems that monitor the plant variables. If they detect that the above-described plant monitoring and control systems have not kept the plant within a predefined set of conditions, they take action automatically to rapidly shut down the plant ("trip" and "scram" are terms that accurately convey the nature of the response) and start any other needed systems to mitigate the detected problem and place the plant in a safe state. These protection and mitigation systems have a number of important characteristics:

(a) They are physically separate systems that generally do not share hardware and software with the plant operating and control systems. (Some limited amounts of equipment such as sensors may be shared provided the equipment meets safety quality requirements.) This extends to and includes needed auxiliary systems such as heating, ventilation, and air conditioning; electrical or hydraulic power supplies; and cooling water systems. (b) They are environmentally qualified for the harshest anticipated operating/accident conditions, including highly unusual events such as large earthquakes and tornadoes. (c) When called upon to act, they go to completion of their intended function. (d) The protection and mitigation systems do not control or modulate the operation of the systems they control. They shut down the reactor, trip the turbine generator, start needed cooling water systems, and go to preset operating conditions that are safe for the plant to maintain for extended periods.

In addition, (e) they are designed to be single-failure proof. That is, no single failure at the component or system level (including a failure internal to the protection and mitigation systems in addition to the initiating event or failure and any direct consequence) or no single operator error can prevent them from successfully operating. As a result, they use *redundancy*. That is, there are typically multiple, separate, parallel sets of equipment and systems to carry out the same function. In the I&C systems in particular, this redundancy is usually provided by having four parallel channels that actuate the systems if needed. The four parallel channels are fed to a logic system that requires any two valid signals to cause actuation. This logic assures that no single failure will prevent or cause the drastic actions taken by these systems. It also allows complete (sensor-to-actuator) testing of one channel at a time while the plant is at power without causing or inhibiting the protection and mitigation function.

In addition to being single-failure proof, (f) the protection and mitigation systems have other features to enhance their reliability and increase their effectiveness against hazards. For example, two reactor shutdown mechanisms are provided—insertion of control rods and injection of a soluble neutron poison. Also, for any given accident, two or more different initiation signals will be generated and sent to the protection and mitigation system. (For example, a loss-of-flow accident through the reactor will be detected by a high reactor outlet temperature and a high pressure signal.) This type of redundancy provides protection against general classes of common-mode failures—failures in which a single error or problem disables multiple, independent safety functions. (Redundancy is discussed further in Chapter 5.)

It is important to note that the requirements of nuclear plant I&C systems, including the protection and mitigation systems, are well within the capabilities of current I&C technology—analog or digital. In terms of response time and accuracy (for example), the nuclear plant I&C requirements are relatively modest.

Safety Systems

The USNRC's safety evaluation of nuclear power plants primarily addresses the protection and mitigation systems. The monitoring and control systems are usually not given credit (see brief discussion of "credit" above) in the hazard and safety analyses of the plants. However, upsets or failures in the monitoring and control systems are usually considered the initiating events for the protection and mitigation systems and, as a result, the USNRC can impose requirements on the monitoring and control systems as well. The monitoring and control systems are also analyzed explicitly in the probabilistic risk assessment (PRA) of each plant to assess how well the plant does in comparison to the USNRC safety goals for nuclear plants. In general, however, the USNRC and the licensing applicant define a set of "safety systems" for each plant, largely comprised of the protection and mitigation systems; it is these safety systems that are subject to the most rigorous licensing and regulatory controls. This is an important distinction because a substantial effort is required to design, qualify, install, test, and maintain these safety systems, and commercial off-the-shelf equipment usually does not meet the requirements. As an indicator, costs of nuclear plant "safety-grade" systems and equipment can be 10 times that of the equivalent commercial quality equipment.

Although this report covers applications of digital I&C systems in nuclear power plants that include all three types—the plant monitoring systems, the plant control systems, and the plant protection and mitigation systems—insofar as the USNRC, the sponsor of this study, is primarily concerned with the "safety-grade" subset of these systems, this report emphasizes this subset.

Operating Conditions for Instrumentation and Control Systems

Nuclear power plant design includes specific consideration of a variety of plant operating conditions. Steady-state, transient, and accident conditions are covered by the regulatory requirements; these requirements also control how and by what criteria the transients and accidents must be analyzed. These analyses, in turn, specify operational requirements the plant equipment and systems must satisfy. For the I&C systems, these specifications include both instrument characteristics (such as input and output range, response time, and accuracy) and the environmental conditions (e.g., temperature, humidity, radiation effects, power supply fluctuations) under which the I&C equipment is required to operate.

Except for the sensors, I&C systems have been specially placed in protected areas so that the environmental conditions they are exposed to are generally rather mild, akin to an "office environment." But the I&C systems must also function in the environment and under the conditions that lead to a transient or accident condition and that develop in the plant as a transient or accident progresses. Because accident conditions typically create a wider and harsher range of operating environments, and because I&C equipment and systems must survive and function in such environments, the equipment and systems must be qualified, usually by test. In general, this harsher operating environment exists only at the sensors and in most of the signal transmission network; the other components are in relatively well-protected (shielded) rooms and benign environments. Most sensors currently employ analog technology. If digital sensors are used, they will have to be designed and tested to show they can withstand these harsher environments.

TRANSITION FROM ANALOG TO DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Background

During their extensive service history, analog I&C systems have performed their intended monitoring and control functions satisfactorily. Although there have been some design problems, such as inaccurate design specifications and susceptibility to certain environmental conditions, the primary concern with the extended use of analog systems is effects of aging, e.g., mechanical failures, environmental degradation, and obsolescence. The industrial base has largely moved to digital-based systems and vendors are gradually discontinuing support and stocking of needed analog spare parts.

Some uses of digital technology in U.S. nuclear power plants go back more than two decades. These early applications were limited but included safety-related applications such as core protection calculators. In the early 1980s, the electronics industry began rapidly shifting to microprocessor-based digital technology. Early implementations of this technology in nuclear plants were successful in reducing unintended plant shutdowns ("trips") and maintenance burdens. This success fueled increased interest in digital applications and provided a training ground for enhancing proficiency and confidence in using digital equipment. At the same time, a number of vendors of instrumentation and control began to reduce their support of the analog equipment, which in turn gave additional practical impetus to the use of digital systems.

The nuclear industry has not been alone. Many other safety-critical industries extensively utilize digital systems. These include aviation and space, chemical-petroleum processing, railroads, defense, and medical applications. These industries face safety issues similar to those faced by the nuclear industry.

The reason for the transition to digital I&C systems[2] lies in their important advantages over existing analog systems. Digital electronics are essentially free of the drift that afflicts analog electronics, so they maintain their calibration better.[3] They have improved system performance in terms of accuracy and computational capabilities. They have higher data handling and storage capacities, so operating conditions can be more fully measured and displayed. Properly designed, they can be easier to use and more flexible in application. They are more widely available. Indeed, digital systems have the potential for improved capabilities (e.g., fault tolerance, self-testing, signal validation, process system diagnostics) that could form the basis for entirely new approaches to achieve the required reliabilities. Because of such potential advantages, and because of the general shift to digital systems and waning vendor support for analog systems, the U.S. nuclear power industry expects substantial replacement of existing, aging analog systems with digital I&C technology. For the same reasons, designs for new, advanced nuclear power plants rely exclusively on digital I&C systems.

In summary, the experience of other safety-critical industries and the increasing age and obsolescence of the existing analog systems suggest that the increasing use of digital I&C technology is inevitable in nuclear power plants. Digital I&C technology is expected to enhance the safety and performance of nuclear power plants by offering process control improvements, such as reduced instrument

[2] The committee intentionally avoided partitioning digital systems between hardware and software; rather the committee believes that digital systems are better treated in an integrated manner. Nevertheless, some of the specific topics addressed in the report merited discussion as "hardware" or "software" items.

[3] The reader should note, however, that since most sensors will remain analog-based, drift will not be eliminated, though it will likely be improved, especially if the digital I&C component contains software specifically designed to offset expected sensor drift.

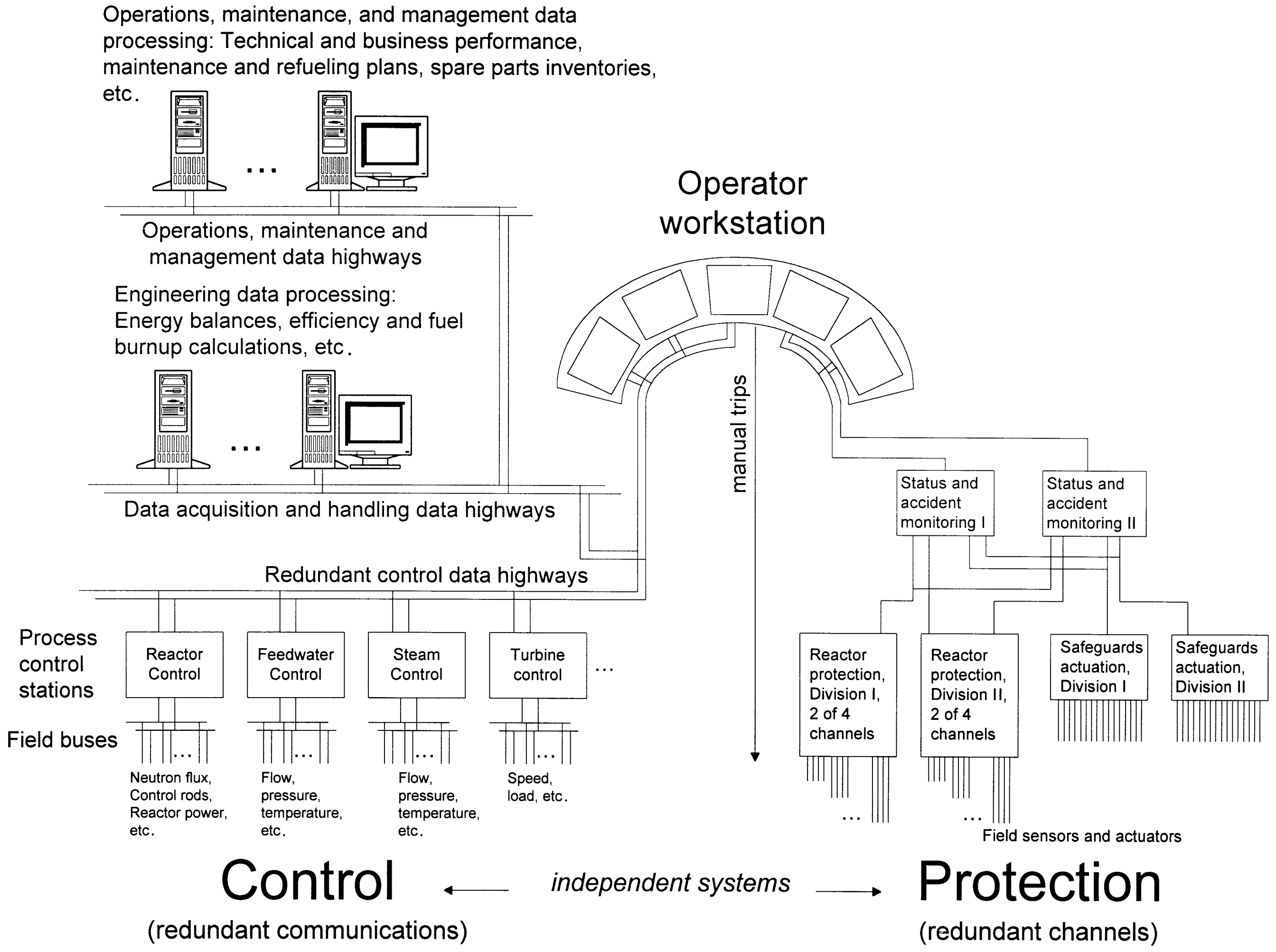
Operations, maintenance, and management data processing: Technical and business performance, maintenance and refueling plans, spare parts inventories, etc.
Operations, maintenance and management data highways
Engineering data processing: Energy balances, efficiency and fuel burnup calculations, etc.
Data acquisition and handling data highways
Redundant control data highways
Operator workstation
manual trips
Status and accident monitoring I
Status and accident monitoring II
Process control stations
Reactor Control
Feedwater Control
Steam Control
Turbine control
Field buses
Neutron flux, Control rods, Reactor power, etc.
Flow, pressure, temperature, etc.
Flow, pressure, temperature, etc.
Speed, load, etc.
Reactor protection, Division I, 2 of 4 channels
Reactor protection, Division II, 2 of 4 channels
Safeguards actuation, Division I
Safeguards actuation, Division II
Field sensors and actuators
Control
(redundant communications)
independent systems
Protection
(redundant channels)

FIGURE 1-1 Illustration of nuclear plant I&C systems.

calibration requirements and improved plant condition monitoring displays (see, e.g., Gill et al., 1994).

Applications to Nuclear Plants

Figure 1-1 illustrates a modern digital I&C system applied to a nuclear power plant. Blocks on the left represent the distributed control systems. These are the systems that are used to regulate plant conditions during startup, power operation, and shutdown. They are responsible for maintaining plant systems and components within their operating ranges, and they normally operate in a regulating mode.

Notice that Figure 1-1 shows redundant data buses in these control systems. These data buses are used to transport the large amounts of information typically handled in a large generating station. The use of data buses reduces and simplifies plant wiring and consequently reduces the requirements for managing and maintaining wiring configuration. Redundancy and separation (including different routing) provides for increased data bus reliability. In this manner, reliable communications can be provided for the large numbers of information data points. Notice also, however, the lower level blocks on the left of Figure 1-1 dedicated to the control of individual systems (such as feedwater control). Real-time control functions are executed in these dedicated modules.

Blocks on the right of Figure 1-1 represent the independent protection (safety) systems. They are responsible for detecting system failures and isolating or shutting down failed systems to protect the plant investment and the public health. This type of system normally uses multiple channels in a voting scheme to trigger the isolation or shutdown action. A typical voting scheme uses a two-out-of-four logic according to which, if one of the four channels fails, the failed channel may be taken out of service for repairs, while still leaving the remaining channels to take action using two-out-of-three logic. Thus, the system is single-failure proof. The use of two channels to trigger an action provides protection against unnecessary spurious trips.

Figure 1-1 also shows point-to-point data links in the protection systems, which provide for more deterministic and predictable data communications for the fewer data points that are normally needed and handled in safety systems. Notice also the independent manual trips bypassing all microprocessor-based systems.

Virtually all of the 109 nuclear power plant units in operation today have digital I&C components. Some of these were part of the original design, for example, digital radiation monitoring equipment and diesel generator sequencers. The earliest implementations used solid-state logic operating at higher and relatively stiffer voltage levels than those of today's microprocessor-based designs. Moreover, these earlier systems did not employ the signal concentrations of multiplexed microprocessor-based systems. Modern systems also employ faster clock speeds, larger memories, and expanded word lengths that have allowed new developments in the software area as well. This in turn has led to heightened interest by the USNRC.

More recently, many plants have retrofitted some I&C components and systems with modern digital technology (ACRS, 1993b). Although many of these retrofits have been relatively small-scale, one-for-one replacements for such components as recorders, meters, and displays, in recent years some relatively large-scale, microprocessor-based, system-level retrofits have been made (Palo Verde Nuclear Generating Station, 1993; Prairie Island Nuclear Generating Plant, 1993; Turkey Point Plant, 1990; USNRC, 1992; USNRC, 1993b). These include:

- reactor protection systems at Northeast Utilities Company's Haddam Neck plant; Tennessee Valley Authority's Sequoyah plant; Commonwealth Edison Company's Zion plant, Unit 2; and Pacific Gas and Electric Company's Diablo Canyon plant
- anticipated transients without scram systems at Arizona Public Service Company's Palo Verde plant, Units 1, 2, and 3
- load sequencers in the emergency power system at Florida Power and Light Company's Turkey Point plant, Units 3 and 4
- station blackout/electrical safeguards upgrades at Northern States Power Company's Prairie Island plant, Units 1 and 2

Applications in Advanced U.S. Plants

In the United States, the advanced reactor designs being developed incorporate all-digital systems intended to utilize and exploit the new technology. They also feature enhanced human-machine interfaces such as more versatile displays with integrated process information (ACRS, 1991). These features, along with the other features of advanced plants, are intended to make the advanced plants simpler and safer. Certification of these designs has been sought (under the provisions of 10 CFR 50.52).

LICENSING OF INSTRUMENTATION AND CONTROL SYSTEMS

Design Guidance

Licensing of any systems for use in a nuclear power plant is governed by formal, documented criteria. These criteria are stated in the General Design Criteria (GDC) (Title 10 CFR Part 50, Appendix A, 1995), which are part of federal law. The GDC are written for I&C systems at a very general level. The GDC were written early in the development of commercial nuclear power, before digital equipment, advanced materials, or modern fire-fighting systems such as halon were used in nuclear plants. The GDC requirements are nevertheless very important in guiding the design of digital systems in nuclear power plants. Examples of requirements from the GDC of particular interest for this report are contained in Appendix E.

In order to make the requirements more specific and useful on a day-to-day basis, the USNRC provides extensive supplemental guidance in a variety of forms (see Table 1-1). For example, numerous regulatory guides have been issued that describe interpretations of the regulations acceptable to the USNRC staff. These "reg guides" are not mandatory, but if they are followed by the licensing applicant they provide a basis upon which the applicant's proposal will be accepted. Other regulatory guidance is provided by endorsement of a wide variety of industry standards and through the promulgation of branch technical positions, which are technical positions adopted by various branches (offices) of the USNRC regulatory staff. Much of this guidance is conveniently summarized in the Standard Review Plan (USNRC, 1981). The Standard Review Plan provides detailed guidance to the USNRC reviewers as to what is needed from the licensee to assess the adequacy of a proposed design; it also defines a satisfactory method of complying with the licensing requirements. (The guidance provided by the regulatory guides, branch technical positions, and industry standards is still more detailed.) A major revision of the Standard

TABLE 1-1 USNRC Design and Quality Assurance Guidance

	Criteria and Supplemental Guidance
Design guidance	Generic design criteria (GDC) Supplemental guidance (summarized in the Standard Review Plan) Regulatory guides Branch technical positions Generic letters Industry standards
Quality assurance	Generic criteria (10 CFR 50, Appendix B) Supplemental guidance Industry standards Other guidance

Review Plan is currently in progress to fully adapt it and the associated regulatory guides, branch technical positions, and USNRC endorsements of industry standards to digital I&C systems.

Note that as a result of all these documents there is a lot of existing high level guidance which is generally accepted and applied. For example, nuclear plants, including the digital I&C systems, are routinely required to undergo extensive hazards analyses as part of the licensing process. The regulators expect and the industry provides formal systematic reviews of the hardware and software using formal requirement specifications and independent reviews. It is not at this high level that additional criteria or guidance is needed. The difficulty arises in trying to implement this high level guidance at the working level and trying to establish a working consensus in particular areas. Consider, for example, common-mode software failure. USNRC regulators require that this problem be addressed and if a potential common-mode failure concern is detected then it must be dealt with. The exact methodology by which potential common-mode failures must be dealt with are not straightforward and there is considerable controversy over what may be appropriate.

Quality Assurance

There are basic requirements for quality assurance. Within the context of these requirements, quality is demonstrated by meeting the Quality Assurance Criteria for nuclear power plants (Title 10 CFR Part 50, Appendix B, 1995) and the related, subsidiary industrial standards, including those on environmental qualifications. These basic requirements are supplemented by more specific regulatory guidance that was originally based on analog equipment but is being revised to specifically address digital equipment in the revision process described above (see Table 1-1).

Modifications and Upgrades

Another important aspect of any system modifications and replacement of existing equipment is 10 CFR 50.59 (see Appendix E), which also applies to I&C systems. The purpose of this regulation is to define the circumstances under which the licensees may, without prior USNRC approval, make changes and conduct experiments and tests that are not specifically provided for in their facility licenses. Since virtually all U.S. nuclear plants have original analog equipment, 10 CFR 50.59 is of particular interest if a licensee is contemplating a digital modification or upgrade. If the criteria for making a change without prior regulatory approval defined under 10 CFR 50.59 are not satisfied, a formal change to the license is needed under another part of the federal code, 10 CFR 50.90. The process required to formally change the license under 10 CFR 50.90 is more difficult procedurally, is more costly, and requires a longer schedule. Cost and schedule become increasingly important as utility companies feel the pressure of increasing economic competition and as proposed investments such as digital upgrades and modifications face stringent economic tests, such as rapid returns on investment.

The conditions an upgrade or modification must meet to be carried out under 10 CFR 50.59 are, first, that it must adhere to the design and operating conditions formally documented in the technical specifications for the license. Second, the change must not result in an "unreviewed safety question" (USQ). The criteria for determining whether or not a USQ exists are stated in 10 CFR 50.59(a)(2) (see Appendix E). To avoid a USQ, the change must not allow (a) an increased probability of occurrence or consequences of an accident or malfunction of equipment important to safety as previously evaluated in the licensing basis (safety analysis report); (b) possible creation of an accident or malfunction of a different type than previously evaluated in the licensing basis; or (c) a reduced margin of safety as defined in the licensing basis for any technical specification.

USNRC regulatory treatment of upgrades or modifications to nuclear power plants may be summarized as follows:

- If there is a change in technical specifications, the licensee must seek prior USNRC approval via 10 CFR 50.90.
- If the licensee's analysis shows the presence of a USQ per 10 CFR 50.59(a)(2), the licensee must seek prior USNRC approval via 10 CFR 50.90.
- If there is no change in technical specifications and no USQ is uncovered, the licensee can make the change or upgrade without prior USNRC approval via 10 CFR 50.59.

There has been continuing discussion and controversy as to exactly how to interpret 10 CFR 50.59 when applied to digital modifications; this is discussed further in this report (see Chapter 9). Nevertheless, many digital retrofits have been made without the creation of a USQ as defined in 10 CFR 50.59 (see Appendix C).

CHALLENGES TO THE INTRODUCTION OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Successful introduction of digital I&C systems into U.S. nuclear power plants faces several challenges. These challenges have several related sources:

Uncertainty Inherent in Introduction of New Technology. There is some uncertainty inherent in the introduction of any new technology. According to Kletz (1995), "all changes and all new technologies introduce hazards as well as benefits." In a safety-critical industry like nuclear power, the users, designers, and regulators must proceed on the basis of choosing and implementing digital modifications so that the current high level of industrial and public safety is at least maintained and preferably increased. The challenge is to take advantage of the performance and safety enhancements potentially available from the use of digital technology without introducing offsetting potential hazards. Further, the design, assessment, and regulatory approach of these new digital systems must also provide some means of assessing the resultant margins of safety.

Shift of Existing Technology Base from Analog Experience. Much of the experience with U.S. nuclear plant design and operation has evolved primarily within the context of analog technology, as has the regulatory framework. Hence, in addition to coping with uncertainties arising from digital technology itself, its use may require changes or additions to the underlying technical infrastructure and regulatory framework.

Technical Problems Identified from Some Applications of Digital I&C in Nuclear Power Plants. The introduction and use of digital systems has not been trouble free. For example, on the basis of recent plant experience with several digital I&C retrofits, the USNRC has identified the following potential problem areas with digital I&C systems (Mauck, 1995):

- common-mode failure in software
- commercial dedication of hardware and software
- possible lack of on-site plant experience with the new technology and systems
- configuration management
- increased complexity leading to possible programming errors and incorrect outputs
- reliability of standard software tools
- environmental sensitivity:[4] electromagnetic or radiofrequency interference, temperature, power quality, grounding, smoke
- effects on plant margin of safety

Similar problems have also occurred in other applications and other industries (Kletz, 1995).

Difficult, Time-Consuming, and Customized Licensing Approach. Licensing of digital technology has presented a particular challenge for the USNRC. Because the regulatory approach has evolved with limited explicit consideration of digital technology, and because the response time to develop new regulatory bases and documentation is long, the pace of change in I&C systems has strained the regulatory process. As a result, the licensing process to date for regulatory review and approval of new digital I&C systems and modifications to existing systems has been difficult, time-consuming, and largely customized for each application.[5] Many utilities are reluctant to seek a change that could not be carried out under 10 CFR 50.59, that is, without prior regulatory approval. (See below for discussion on recent USNRC activities in the digital I&C licensing process.)

Lack of Consensus (between the USNRC and the Regulated Industry) on Issues Underlying Evaluation and Adoption of Digital I&C Technology and Means to Obtain a Satisfactory Resolution. In order to deal effectively with these challenges, an effective consensus needs to exist. This will allow the benefits of the new technology to be fully exploited while assuring that safety and public confidence are maintained. However, the industry and regulators have less experience with this somewhat unfamiliar technology and have had difficulty in reaching an effective consensus.

It is important to note that the lack of consensus is not about the use of digital systems per se. Rather, much of the controversy revolves around specific issues, e.g., the potential for common-mode failures, and the lack of consensus on these specific issues tends to cloud whether or not the overall advantages of using digital I&C in nuclear power plants outweigh the disadvantages. This is made more difficult by the fact that the U.S. commercial nuclear power industry is heavily regulated. The rules for design and evaluation are subject to legal scrutiny and interpretation with severe penalties for violations and very real possibilities for litigation. Further, there are large amounts of capital investment at stake. Hence, delays in resolving issues, if translated into delays in allowing a nuclear power plant to operate, can cost up to hundreds of thousands of dollars per day. As a result, the definition of licensing criteria must follow systematic study and evaluation and sound synthesis of differing technical viewpoints. It is a process not to be undertaken lightly.

RESPONSE OF THE U.S. NUCLEAR REGULATORY COMMISSION AND NUCLEAR INDUSTRY TO THE CHALLENGES

Activities of the U.S. Nuclear Regulatory Commission

The USNRC has reviewed a number of retrofits of plant I&C systems from analog to digital. It has also begun reviewing designs of advanced plants (USNRC, 1991). However, the review process for both retrofits and advanced plant designs has been customized for each application. This, in turn, has provoked criticism of the USNRC for failing to

[4] Whether the new digital equipment is in fact more sensitive to environmental challenges than existing analog equipment is controversial.

[5] The actual incremental cost and time required for a digital system upgrade is difficult to define and not well agreed upon. Some utilities have told the committee that they budget six months to a year and, for a major modification, incremental costs of a half-million to several million dollars for the regulatory review process. USNRC staff members have told the committee that they take exception to these values and that they expect much shorter times for future reviews.

adopt generically applicable standards. In an effort intended to address this criticism, the USNRC has a process under way to systematically review its internal directives and guidelines governing reviews of I&C systems with a view to adapting them for digital I&C technology (Wermiel, 1995). This process is due to be completed in 1997. In the interim, the USNRC has provided case-by-case approvals in specific plants, sought suggestions by its advisory committees for taking broad action, held a workshop seeking consensus on a regulatory program, and conducted research linking regulatory decision making to the context of I&C technology. A brief account follows. (A more detailed discussion appears in Appendix C.)

Small digital I&C upgrades have been routinely accepted; large retrofits have also been made but the review process has been more difficult. These reviews have led to approvals at a number of nuclear power plants (see, e.g., USNRC, 1993b). Reviews of designs for advanced plants are also in progress. For example, a final design approval of the System 80+ advanced plant design has been completed (USNRC, 1994a).

The USNRC and its staff receive advice from a number of advisory committees. The Advisory Committee on Reactor Safeguards (ACRS), established by Congress in 1957, provides advice to the USNRC on safety aspects of current and planned nuclear facilities and the adequacy of safety standards. It has a subcommittee that examines the use of computers in nuclear power plant operations. The USNRC's Office of Nuclear Regulatory Research conducts a research program to support the organization's regulatory decision making. This program includes areas of focus relevant to the problem of evaluating and regulating digital I&C technology in nuclear power plants. The Nuclear Safety Research Review Committee (NSRRC) is a 12-member group of experts who advise the USNRC's Office of Nuclear Regulatory Research on the quality and management of its research program.

The ACRS and NSRRC have both expressed concern that the USNRC staff may be lagging behind the nuclear industry, in both the United States and foreign countries, in their understanding of the application of digital I&C systems. These committees have also urged the development of an overarching framework to guide USNRC regulation of new digital I&C technology (see, e.g., ACRS, 1992a, 1993a). The ACRS examined digital I&C technology and identified several concerns (ACRS, 1994), including:

- the lack of a coherent and effective review plan, including acceptance criteria, for digital I&C technology
- the need to address software specification development, software verification and validation,[6] environmental effects on hardware, diversity as protection against common-mode failure,[7] and prediction of I&C reliability.

The NSRRC (1992) has expressed concerns that partially overlap with those of the ACRS, such as:

- the need to develop criteria for such issues as hardware reliability, software verification and validation, environmental effects (e.g., electromagnetic interference), common-mode failure, configuration management,[8] and systems integration
- the need for an overarching strategy to guide regulatory developments and the certification process for the new technology
- the rapid pace of technological changes that affect I&C systems, including developments in the areas of artificial intelligence, expert systems, neural networks, fuzzy logic, genetic algorithms, and chaos theory

To address technical concerns, and in hopes of developing a wide consensus across the USNRC and the nuclear industry for a regulatory program, the USNRC held a workshop on digital systems reliability and nuclear safety, cosponsored by the National Institute of Standards and Technology, in September 1993 (USNRC, 1993a).

Activities of the Nuclear Power Industry

The nuclear power industry has been actively addressing the introduction of digital I&C technology into nuclear power plants. Under the auspices of the Electric Power Research Institute (EPRI), the industry has developed guidelines for streamlined licensing of digital I&C upgrades (EPRI, 1993). These guidelines have recently been partially endorsed by the USNRC, subject to specific clarifications (USNRC, 1995). Recent attempts at further clarifications suggest that the USNRC staff position continues to evolve (see Chapter 9 of this report).

The industry has also prepared a "Utility Requirements Document" for advanced plant designs (EPRI, 1992a, 1992b). Chapter 10 of this document provides guidance for designing the digital I&C systems and associated human-machine interfaces for the next generation of nuclear power plants. The document requires the use of fully integrated digital I&C technology. An extensive USNRC review of this

[6] The verification and validation process ensures the adequacy of software requirements and specifications, the adequacy of the software development process, and the compliance of the resultant software with the original specifications.

[7] Common-mode failure is the failure of multiple components in the same way. Common-mode failures arise when the assumption of independence of the failures of the components is violated. Common-mode failures are a concern when the failures occur concurrently or at least sequentially in a time frame before the minimum number of channels is recovered.

[8] As defined in ANSI/IEEE Standard 610.12–1990, configuration management is a discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

document (USNRC, 1994b) did not resolve basic issues inherent in digital I&C technology implementation. However, the USNRC review did produce a set of agreed-upon high-level criteria for advanced plant designs, as well as defining the process the USNRC would use to complete their review and approval of these designs. The USNRC did accept digital technology for all the I&C systems of the advanced nuclear plants. However, for the advanced plants, the detailed issues that are being addressed in existing plants have yet to be addressed.

Other industry efforts include those of the nuclear steam supply system vendors, each of which has an ongoing program for developing digital I&C systems, both for retrofits and upgrades in existing plants and for future plants.

Developments Overseas

There is worldwide interest in digital I&C technology for nuclear power plants. For example, there is already significant application of digital I&C technology to nuclear power plants in Canada, Japan, and Western Europe (ACRS, 1992b; White, 1994). The Canadians have extensive operating experience with digital systems. Digital systems were first implemented 25 years ago because they were better suited to provide on-line control of their natural uranium-fueled, heavy water-moderated (“CANDU”) plants, specifically, to monitor and control the power level and xenon oscillations. The British have adopted digital-based systems throughout their latest plant, Sizewell-B, and they have operated without incident during the first six months of plant operation (Nucleonics Week, 1995). The French have proceeded by gradually and systematically expanding the use of digital systems in each subsequent generation of their highly standardized plants. The latest design is completely digital-based and is implemented in the N4 series, the first of which is located at the Chooz-B site (Nucleonics Week, 1995). In Japan, digital systems have been implemented in several existing plants, including Ohi 3, which started commercial operation in 1992. The most recent plant to go into operation in Japan, the ABWR located at the Kashawazaki site, is a digital-based design.

In addition, the United States, through both the Department of Energy and the USNRC, participates in international collaborative programs such as the Halden Reactor Project of the Organization of Economic Cooperation and Development.

Standards Development

A number of standards, USNRC regulations and regulatory guidelines (see, for example, USNRC, 1981), and USNRC publications exist to guide licensing of the current analog I&C systems. Since they were developed for analog systems, they can be difficult to apply and interpret for digital I&C systems. Nevertheless, pending the extensive revision of the USNRC’s applicable documentation, which is currently under way, these documents have been used for reviewing digital I&C systems.

Standards developed for digital I&C systems in nuclear power plants exist. These include International Electrotechnical Commission (IEC) Standard 880, Software for Computers in the Safety Systems of Nuclear Power Plants (1986); and IEC Standard 987, Programmed Digital Computers Important to Safety for Nuclear Power Plants. A U.S. standard also exists, IEEE 7-4.3.2, Application Criteria for Programmable Digital Computer Systems in Nuclear Power Generating Stations (1993), promulgated by the Institute of Electrical and Electronics Engineers. While not yet formally endorsed by the USNRC, this standard has been employed in the safety evaluation of digital I&C retrofits in nuclear power plants.

THIS STUDY

Committee’s Task

The National Research Council was asked by the USNRC to conduct a study (including a workshop) on application of digital I&C technology to commercial nuclear power plant operations. The National Research Council appointed a committee (hereafter the committee) to carry out the study in two phases. In Phase 1, the committee was charged to define the important safety and reliability issues (concerning hardware, software, and human-machine interfaces) that arise from the introduction of digital instrumentation and control technology in nuclear power plant operations, including operations under steady-state, transient, and accident operating conditions (NRC, 1995).

In response to this charge the committee identified eight key issues associated with the use of digital I&C systems in existing and advanced nuclear power plants. The eight issues separate into six technical issues and two strategic issues. The six technical issues are: systems aspects of digital I&C technology; software quality assurance; common-mode software failure potential; safety and reliability assessment methods; human factors and human-machine interfaces; and dedication of commercial off-the-shelf hardware and software. The two strategic issues are the case-by-case licensing procedure and adequacy of the technical infrastructure. The committee recognizes these are not the only issues and topics of concern and debate in this area. Nevertheless, the committee believes that developing consensus on these key issues will be a major step forward and accelerate the appropriate use and licensing of digital I&C systems in nuclear power plants. These issues were presented in the Phase 1 report. Both the USNRC (represented by the staff of the Office of Nuclear Regulatory Research and the Office of Nuclear Reactor Regulation) and the Advisory Committee on Reactor Safeguards expressed agreement that these were important issues and that work by the committee in Phase 2 in helping arrive at a satisfactory resolution of these issues would be very useful.

In Phase 2 of the study, the committee was charged to identify criteria for review and acceptance of digital I&C technology in both retrofitted reactors and new reactors of advanced design; characterize and evaluate alternative approaches to the certification or licensing of this technology; and, if sufficient scientific basis existed, recommend guidelines on the basis of which the USNRC can regulate and certify (or license) digital I&C technology, including means for identifying and addressing new issues that may result from future development of this technology. In areas where insufficient scientific basis exists to make such recommendations, the committee was to suggest ways in which the USNRC could acquire the required information.

In carrying out its Phase 2 charge, the committee limited its work to those issues identified in Phase 1. The issues were chosen because they were difficult and controversial. Further, the committee recognized that by law, the responsibility for setting licensing criteria and guidelines for digital I&C applications in nuclear plants rests with the USNRC. Thus, the reader should not form too literal an expectation that the committee has provided a cogent set of principles, design guidelines, and specific requirements for ready use by the USNRC to assess, test, license, and/or certify proposed systems or upgrades. Rather, the results of the study are presented not in the form of simple generic criteria statements (i.e., at a high level of elaboration) but in the form of conclusions and recommendations related to each issue and primarily addressed to the USNRC for their consideration and use. In the committee's view, there is substantial further work to be accomplished. The committee expects the USNRC and the nuclear industry to extend the work of criteria development beyond where this Phase 2 report leaves it. To guide further work on the eight key issues studied, the committee's report offers findings and recommendations in four broad categories: (a) current practice (of the USNRC and the U.S. commercial nuclear industry) that is essentially satisfactory or requires some fine tuning, (b) points of weakness in the USNRC's approach, (c) issues that merit further inquiry and research before satisfactory regulatory criteria can be developed, and (d) criteria and guidelines that are unreasonable to expect in the near future.

Conduct of the Study

In conducting its study, the committee reviewed a large number of documents made available by the USNRC and a variety of other sources. The committee also interviewed selected personnel from the USNRC, from the two advisory committees discussed above (ACRS, NSRRC), from the nuclear industry, and from other industries using digital systems in safety-critical applications. The committee also sought the view of individuals from academia and research organizations. In addition, the committee visited control room simulators, a nuclear plant, and a fossil-fueled power plant with extensive digital I&C systems (see Appendix B). The committee also had frequent and detailed internal discussions, both face-to-face and via paper and electronic communications. The committee also brought to bear a wide range of experience in and knowledge of the field (see Appendix A).

Carrying Out the Charge

The committee took seriously the charge that it identify criteria for review and acceptance of digital I&C technology and that it recommend guidelines for regulation and certification. In carrying out its charge, the committee recognized that:

- In order to develop useful guidance, only a limited number of issues could be dealt with in the relatively brief duration of the study.
- General, high level criteria would not be particularly useful.
- The final criteria are legally the USNRC's responsibility. Further, since the nuclear power industry is heavily regulated in the public interest, the licensing criteria should be forged in a detailed interaction among the regulators, the industry, and the public.
- The committee has a wide range of expertise and experience in digital systems and nuclear power plants but it is not a surrogate for this interaction among the stakeholders. Hence, the committee could serve by clearly delineating and defining issues and providing guidance for resolving these issues rather than developing specific licensing criteria.

Accordingly, the committee selected eight issues for study and worked on those issues. These eight issues address the two major intertwined themes associated with the use of digital instrumentation and control in nuclear power plants. These are:

1. Dealing with the specific characteristics of digital I&C technology as applied to nuclear power plants.
2. Dealing with a technology that is more advanced than the one widely in use in existing nuclear power plants. This technology is rapidly advancing at a rate and in directions largely uncontrolled by the nuclear industry but at the same time likely to have a significant impact on the operation and regulation of the nuclear industry.

The technical issues of this report are primarily related to digital technology itself (Theme 1) while the strategic issues are primarily related to the process of adopting advanced technology (Theme 2). The committee concentrated on reviewing the current approaches being taken by the nuclear industry and its regulators toward dealing with the selected key issues. The committee also tried to learn from the experience of the international nuclear industry as well as gather and evaluate information about how other safety-critical industries and their regulators dealt with these issues. Also, through the technical expertise and knowledge of its various members, the committee explored work done by the digital systems community at large, including both research activities and academic work.

As the committee worked through the issues it discovered there is a major impediment to progress. This is the communication barriers that exist among the key technical communities and individuals involved. The basic reason for the communication difficulty is apparent. Work is simultaneously going on in many areas, each with its own technology, research focus, and agenda. Unfortunately, although many of these areas use common terms, these terms often have different meanings to different groups, resulting in either a lack of communication or very difficult communication. This is particularly troublesome for the nuclear power industry and its regulators, who are not dominant in this technology and must try to synthesize information and experience from a variety of sources and apply it in power plants where safety hazards must be dealt with in a rigorous way, under public scrutiny. In Chapter 11 the committee discusses this communication problem in more detail and provides suggestions for a way forward. Making substantial progress in this area should have a multiplicative effect as it eases the resolution of many specific technical and strategic issues.

Overall, while there are important steps that remain to be taken by the USNRC and industry as addressed in this report, the committee found no insurmountable barriers to the use of digital instrumentation and control technology to nuclear power plants. The committee also believes that a forward-looking regulatory process with good and continuing regulations and industry communication and interaction will help. All participants must recognize that crisp, hard-edged criteria are particularly difficult to come by in this rapidly moving area and good practices and engineering judgment will continue to be needed and relied upon.

For the key technical issues (systems aspects of digital I&C technology; software quality assurance; common-mode software failure potential; safety and reliability assessment methods; human factors and human-machine interfaces; and dedication of commercial off-the-shelf hardware and software) the committee provides specific recommendations and conclusions which include a number of specific criteria. These are listed in each chapter (see Chapters 3 through 8). But recognizing the difficulty of defining specific criteria, and the need for the nuclear technology stakeholders, particularly the USNRC, to make the final decisions, the committee focused on (a) providing process guidance both in developing guidelines and in the short-term acceptance of the new technology; (b) identifying promising approaches to developing criteria and suggestions for avoiding dead-ends; and (c) mechanics for improving communication and strengthening technical infrastructure.

For the key strategic issues (the case-by-case licensing procedure and adequacy of the technical infrastructure) the committee:

- Emphasizes guidance to implement a generically applicable framework for regulation that follows current USNRC practice and which in particular draws a distinction between major and minor safety modifications. The committee also provides guidance for the evaluation and updating of this regulatory framework (see Chapter 9).
- Identifies a need to upgrade the current USNRC technical infrastructure and suggests specific research activities that will support the needed regulatory program and USNRC's research needs. The committee also suggests several improvements to the technical infrastructure to improve and maintain technical capabilities in this rapidly moving, technically challenging area.

The specific recommendations made by the committee thus offer guidance toward implementing and maintaining the currency of a generically applicable framework for regulation that follows current USNRC practice and draws a distinction between major and minor safety modifications. The committee suggests specific research activities that will support this program and makes a number of suggestions for improving USNRC capabilities for addressing these issues.

Contents of This Report

This report contains 11 chapters and six short appendices. Chapter 1 (this chapter) briefly discusses the scope, basis, and context for the study. Chapter 1 also discusses use of digital I&C systems in nuclear plants in some detail so the reader has the necessary background to follow the more detailed discussions and evaluations in the remainder of the report. Chapter 2 briefly describes how the original issues were derived and places the specific issues in overall context, explaining their interrelationships and the relative priorities assigned to them by the committee. Chapters 3 through 10 discuss each of the individual issues in turn. The detailed discussions in these chapters include the committee's conclusions and recommendations regarding each issue. Chapter 11 presents an overview and summary of the committee's findings. Appendices A through F provide useful information too detailed to include in the body of the text.

REFERENCES

ACRS (Advisory Committee on Reactor Safeguards to the U.S. Nuclear Regulatory Commission). 1991. Minutes of ACRS Subcommittee Meeting on Computers in Nuclear Power Plant Operations, February 6, 1991. Washington, D.C.

ACRS. 1992a. Digital Instrumentation and Control System Reliability. Letter to I. Selin, Chairman, USNRC, September 16, 1992. Washington, D.C.

ACRS. 1992b. Minutes of ACRS Subcommittee Meeting on Computers in Nuclear Power Plant Operations: Special International Meeting, September 22, 1992. Washington, D.C.

ACRS. 1993a. Computers in Nuclear Power Plant Operations. Letter to I. Selin, Chairman, USNRC, March 18, 1993. Washington, D.C.

ACRS. 1993b. Minutes of ACRS Subcommittee Meeting on Computers in Nuclear Power Plant Operations: Quantitative Software Assessment and Analog-to-Digital Industry Experience, February 9, 1993. Washington, D.C.

ACRS. 1994. Proposed National Academy of Sciences/National Research Council Study and Workshop on Digital Instrumentation and Control Systems. Letter to I. Selin, Chairman, USNRC, July 14, 1994. Washington, D.C.

EPRI (Electric Power Research Institute). 1992a. Advanced Light Water Reactor Utility Requirements Document. EPRI NP-6780-L. Palo Alto, Calif.

EPRI. 1992b. Advanced Light Water Reactor Utility Requirements Document. EPRI NP-6780-L, Vol. 2 (ALWR Evolutionary Plant) and Vol. 3 (ALWR Passive Plant), Ch. 10: Man-Machine Interface Systems. Palo Alto, Calif.: EPRI

EPRI. 1993. Guideline on Licensing Digital Upgrades. EPRI TR-102348. Palo Alto, Calif.: EPRI

Gill, W., D. Harmon, T. Rozek, and S. Wilkosz. 1994. Nuplex 80+ Advanced Control Complex: Enhanced Safety Through Digital Instrumentation and Control. 9th Annual Korean Atomic Industrial Forum and Korean Nuclear Society (KAIF/KNS) Conference, April 6–8, 1994.

Kletz, T. 1995. Computer Control and Human Error. Houston: Gulf Publishing.

Mauck, J. 1995. Regulating Digital Upgrades. Presentation to the Committee on Applications of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., January 31.

NRC (National Research Council). 1995. Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Phase 1. Board on Energy and Environmental Systems, National Research Council. Washington, D.C.: National Academy Press.

NSRRC (Nuclear Safety Research Review Committee to the U.S. Nuclear Regulatory Commission). 1992. Summary of April 29, 1992, Meeting. Letter to E. Beckjord, USNRC, November 16, 1992. Washington, D.C.

Nucleonics Week. 1995. Outlook in I&C: Special Report to the Readers of Nucleonics Week, Inside the N.R.C. and Nuclear Fuel. September and October.

Palo Verde Nuclear Generating Station. 1993. NRC Inspection Report 50-528, 50-259, and 50-530/93-07 Related to Amendment to Operating Licenses No. NPF-41, NPF-51, and NPF-74, Implementation Inspection for Anticipated Transients Without Scram (ATWS) Systems: Palo Verde Nuclear Generating Station Units 1, 2, and 3. Dockets Nos. 50-528, 50-529, and 50-530, April 9, 1993. Washington, D.C.

Prairie Island Nuclear Generating Plant. 1993. Supplemental Safety Evaluation by the Office of Nuclear Reactor Regulation: Revision 1 of Design Report for Station Blackout/Electrical Safeguards Upgrade Project, Amendment to Facility Operating License No. DPR-42 and DPR-60: Prairie Island Nuclear Generating Plant, Units 1 and 2. Dockets Nos. 50-282 and 50-306, January 4, 1993. Washington, D.C.

Title 10 CFR (Code of Federal Regulations) Part 50, Appendix A. 1995. General Design Criteria for Nuclear Power Plants.

Title 10 CFR Part 50, Appendix B. 1995. Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

Turkey Point Plant. 1990. Safety Evaluation Report by the Office of Nuclear Reactor Regulation of the Load Sequencers in the Enhanced Power System at Turkey Point Plant, Units 3 and 4, Amendment to Operating Licenses DPR-31 and DPR-41, Dockets Nos. 50-250 and 50-251, November 5, 1990. Washington, D.C.

USNRC (U.S. Nuclear Regulatory Commission). 1981. USNRC Standard Review Plan (SRP), NUREG-0800, section 7.1, Instrumentation and Controls. Other sections applicable to instrumentation and control technology include: 3.10, Seismic and Dynamic Qualification of Mechanical and Electrical Equipment; 3.11, Environmental Qualification of Mechanical and Electrical Equipment; 4.4, Thermal and Hydraulic Design; 7.2, Reactor Trip System; 7.3, Engineered Safety Features Systems; 7.4, Safe Shutdown Systems; 7.5, Information Systems Important to Safety; 7.6, Interlock Systems Important to Safety; 7.7, Control Systems; 8.1, Electric Power; 8.2, Offsite Power System; 8.3.1, A-C Power Systems (Onsite); 8.3.2, D-C Power Systems (Onsite); 15.0, Review of Anticipated Operational Occurrences and Postulated Accidents; 15.1.5, Steam System Piping Failures Inside and Outside of Containment. Washington, D.C.: USNRC.

USNRC. 1991. Digital Computer Systems for Advanced Light Water Reactors. USNRC SECY-91-292. Washington, D.C.: USNRC.

USNRC. 1992. Safety Evaluation Report Related to Amendment No. 127 to Facility Operating License No. DRP-48: Zion Nuclear Power Station, Unit 2. Docket No. 50-304, June 9, 1992. Washington, D.C.: USNRC.

USNRC. 1993a. Proceedings of the Digital Systems Reliability and Nuclear Safety Workshop, U.S. Nuclear Regulatory Commission, September 13–14, 1993, Gaithersburg, Md. NUREG/CP-0136. Washington, D.C.: U.S. Government Printing Office.

USNRC. 1993b. Safety Evaluation Report by the Office of Nuclear Reactor Regulation Related to Amendment No. 84 to Facility Operating License No. DPR-80 and Amendment No. 83 to Facility Operating License No. DPR-82: Eagle 21 Reactor Protection System Modification with Bypass Manifold Elimination: Diablo Canyon Power Plant. Dockets Nos. 50-275 and 50-323, October 7, 1993. Washington, D.C.: USNRC.

USNRC. 1994a. Final Safety Evaluation Report: Related to the Certification of the System 80+ Design. NUREG-1462, Vols. 1–2. Washington, D.C.: USNRC.

USNRC. 1994b. NRC Review of Electric Power Research Institute Advanced Light Water Reactor Utility Requirements Document. NUREG-1242, Vol. 3, Parts 1–2. Washington, D.C.: USNRC.

USNRC. 1995. Use of NUMARC/EPRI Report TR-102348, “Guideline on Licensing Digital Upgrades,” in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59. NRC Generic Letter 95-02. Washington, D.C.: USNRC.

Wermiel, J. 1995. Update of Instrumentation and Control Systems Section of the Standard Review Plan, NUREG-0800. Presentation to the Advisory Committee on Reactor Safeguards to the U.S. Nuclear Regulatory Commission, Rockville, Md., April 7.

White, J. 1994. Comparative Assessments of Nuclear Instrumentation and Controls in the United States, Canada, Japan, Western Europe, and the Former Soviet Union. JTEC/WTEC Annual Report and Program Summary 1993/94. Baltimore, Md.: World Technology Evaluation Center, Loyola College.

2

Key Issues

Digital instrumentation and control systems for nuclear power plants have very similar technological characteristics—the equipment, response time, input and output range, and accuracy—to digital instrumentation and control systems for other safety-critical applications such as chemical plants and aircraft. What distinguishes digital I&C (instrumentation and control) applications in nuclear power plants from other digital I&C applications is the need to establish very high levels of reliability under a wide range of conditions. Because of the potentially far greater consequences of accidents in nuclear power plants, the I&C systems must be relied upon to reduce the likelihood of even low-probability events. The U.S. Nuclear Regulatory Commission (USNRC) has developed a regulatory process with the goal of achieving these high levels of reliability and thus assuring public safety. This process is subject to public scrutiny.

DEVELOPING THE KEY ISSUES (PHASE 1)

In Phase 1 of the study, the committee identified eight key issues associated with the use of digital I&C systems in existing and advanced nuclear power plants. In the committee's view, these issues need to be addressed and a working consensus needs to be established regarding these issues among designers, operators and maintainers, and regulators in the nuclear industry. The process the committee followed to identify these issues in Phase 1 is discussed in the Phase 1 report (NRC, 1995) and is only briefly summarized here.

In essence, the committee considered the impact of digital I&C systems against a set of standard regulatory approaches to assessing and ensuring safety (defense-in-depth, safety margins, environmental qualification, requisite quality assurance, and failure invulnerability). From this analysis, the committee identified a number of questions, issues, and facets of issues (see Appendix D). After a number of deliberations, the committee winnowed the list down to eight key issues.

The eight issues separate into six technical issues and two strategic issues. The six technical issues are systems aspects of digital I&C technology, software quality assurance, common-mode software failure potential, safety and reliability assessment methods, human factors and human-machine interfaces, and dedication of commercial off-the-shelf hardware and software. The two strategic issues are the case-by-case licensing process and the adequacy of technical infrastructure (i.e., training, staffing, research plan). The committee recognizes that these are not the only issues and topics of concern and debate in this area (see Appendix D). Nevertheless, the committee reaffirms its judgment, initially formed during Phase 1, that developing a consensus on these eight issues will be a major step forward and accelerate the appropriate use and licensing of digital I&C systems in nuclear power plants.

At the end of Phase 1, it became clear to the committee that the software-related issues and the regulating process would be particularly challenging aspects of the study. Accordingly, the committee strengthened its capability by adding to its numbers two experts in these areas (see Appendix A).

ADDRESSING THE KEY ISSUES (PHASE 2)

In Phase 1, the committee largely operated as a single group. In approaching Phase 2, the committee recognized that deeper study of each issue would be needed to provide a firm foundation for developing specific conclusions and recommendations. The committee accordingly formed working subgroups associated with each area. These subgroups, each led by a member of the committee particularly knowledgeable in that area, were charged with studying the issues in detail, developing topic papers, identifying and reviewing key reference documents, and arranging for presentations by those active in the field to the full committee. However, the committee recognized that several issues had close interrelations, requiring that the committee also work as an integrated body to achieve a balanced perspective and forge a committee consensus. Thus, each issue received significant attention by the entire committee.

PRESENTING THE KEY ISSUES

The issues are discussed individually in Chapters 3 through 10 of this report. The committee has maintained the separation between technical issues and strategic issues in the Phase 2 report, even though as work proceeded in Phase 2 it became increasingly apparent that the technical issues and the strategic issues are tightly interwoven. The technical issue discussions (Chapters 3 through 8) generally focus on the technical basis of the issue and how pertinent technical knowledge (or the lack thereof) affects how the issue is addressed in U.S. nuclear plants, foreign plants, and other industries and their regulators. For each issue, the committee draws conclusions and provides recommendations.

Discussion of the two strategic issues (Chapters 9 and 10) focuses on the licensing process and a key underlying area, the way in which the USNRC has developed and continues to develop its technical infrastructure (staffing, training, and research plans) in the digital I&C area. In Phase 1, the committee became convinced that even if the six technical issues were resolved and no controversy or lack of consensus existed, these strategic issues would still need to be carefully considered and addressed. Concern with these two strategic issues reflects the recognition that rapidly moving and evolving technologies present a special difficulty for an industry and its regulators where licensing and certification processes generally move more slowly than the technology they are intended to regulate.

Because the issues are highly interrelated and are relatively general, the committee debated their relative importance and their order of presentation, which warrants the following brief discussion of their arrangement in this report.

The committee chose to present the technical issues first to provide a basis and context for the strategic issues presented later. Of all the technical issues, systems aspects of digital I&C technology is addressed first (in Chapter 3) because it is a broad issue that encompasses many others. Next (in Chapters 4, 5, and 6), the committee has chosen to present the three issues primarily related to software.[1] Software constitutes a major difference between analog and digital I&C applications, and its use raises some concerns. Software is a design artifact and, because it is, there is difficulty showing definitively that it has no critical errors. Software is also more amenable to the addition of features and enhancements (so-called "creeping complexity") not needed for its basic function, whereby the system becomes more difficult to understand. As the most general of the three software issues, software quality assurance is discussed first (Chapter 4). The issue of software common-mode failures is discussed next (Chapter 5). Common-mode failure in software is closely related to software quality assurance but warrants discussion as a separate topic because of its significance to the safety-critical digital applications, with their emphasis on independence, redundancy, and diversity. The final issue discussed in the primarily software-related group is quantitative safety and reliability assessment methods (Chapter 6).

The committee then turns to the issue of human factors and the human-machine interface (Chapter 7), an issue important in both analog and digital systems. Digital I&C technology has the potential to greatly improve the human factors and human-machine interfaces so that the combination of the human operator and the computer could provide greatly improved process control and enhanced safety. There are, however, unique design challenges that digital technology I&C presents.

The last technical issue discussed is dedication and use of commercial off-the-shelf (COTS) digital I&C systems and equipment in nuclear power plants (Chapter 8). This topic is important because much of the existing I&C equipment in nuclear power plants is becoming obsolete and vendor support is waning. The nuclear plant market is relatively small and COTS offers a potentially cost-effective way to address this problem. Other industries have reached the same conclusion and are reportedly finding some success (Loral, 1996). This is a relatively new area for nuclear plants, particularly in safety system applications, but there is considerable industry activity and regulatory involvement.

Finally, the committee turns to the two strategic issues, case-by-case licensing and adequacy of the technical infrastructure (discussed in Chapters 9 and 10). Both the Advisory Committee on Reactor Safeguards and the Nuclear Safety Research Review Committee share the committee's view that successful resolution of these issues is a necessary prerequisite to successfully applying digital I&C systems in nuclear power plants.

[1] In its internal discussions, however, the committee arrived at the view that in general the software and hardware aspects of a digital application cannot be clearly separated.

REFERENCES

Loral (Loral Space Information Systems). 1996. Mission Control Center Upgrade at NASA Johnson Space Center. Houston, Texas: Loral Corporation press release.

NRC (National Research Council). 1995. Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Phase 1. Board on Energy and Environmental Systems, National Research Council. Washington, D.C.: National Academy Press.

3

Systems Aspects of Digital Instrumentation and Control Technology

INTRODUCTION

Digital instrumentation and control (I&C) systems have proven to be useful and beneficial in a wide range of applications including fossil-fueled power generation, electric power distribution, petroleum refining, petrochemical production, aerospace, and some nuclear power plant applications (e.g., core protection calculators, diesel generator load sequencers, a few digital reactor protection systems, and plant radiation monitoring systems). This usefulness is evidenced by the trend over the last 20 years toward investment in digital I&C applications in the process industries.

However, digital I&C systems were not an instant success; early on it became clear that careful attention to systems aspects[1] would be necessary to avoid unanticipated failure modes. In the late 1960s, there was mixed success using central computers in the so-called "direct digital control" architecture (commonly referred to as DDC) for process control. A transition was soon made to the so-called "supervisory control" architecture, in which minicomputers were used to transmit "supervisory" commands to analog controllers that performed continuous process regulation.

Eventually, this transition led to today's modern multilayered architectures in which (a) local controllers perform component control functions, (b) higher- (system-) level control stations coordinate in a supervisory mode the operations of multiple components in a system or multiple systems in a unit, and (c) higher-level stations perform plant-level supervisory functions and data analyses.

There are many options by which to implement these architectures. Selecting among these options involves addressing considerations such as (a) allocations of functions to different layers of the system, and to hardware and to software; (b) communications schemes within and between layers; (c) methods for achieving timely execution of data acquisition, analyses, and control functions; and (d) provisions for redundancy and diversity. One possible application of such a multilayered architecture to a nuclear generating station is described in Chapter 1 of this report (see Figure 1-1). Notice in Figure 1-1 the multiple horizontal layers of functionality that are typical in today's digital I&C systems, along with the traditional nuclear plant features of vertical independence between protection and control and the use of independent manual backup trips. Figure 1-1 also illustrates the use of redundancy in sensing and communication lines and the extensive use of data buses in the control system compared to the extensive use of deterministic point-to-point communications in the protection system.

Recent experience with large-scale, fully integrated digital I&C systems at nuclear power plants has also had its difficulties. There have been problems, apparently related to systems aspects, that have caused substantial delays and increased costs. In addition, there is increasing use of open systems, in which multiple vendors provide components that must successfully interact. Open systems are used because they foster competition and standardization and avoid dependence on single suppliers. However, the presence of multiple vendors may make successfully dealing with systems aspects more difficult because of the increased number of interfaces.

Statement of the Issue

Along with important benefits, digital I&C systems introduce potential new failure modes that can affect operations and margins of safety. Therefore, digital I&C systems require rigorous treatment of the systems aspects of their design and implementation.[2] What methods are needed to address this concern? How can the experience and best practices of the various technical communities involved in applying digital I&C technologies be best integrated and applied to nuclear power plants? What procedures can be put

[1] "Systems aspects" refers to those issues that transcend the particular component(s) that comprise the system and possibly even the function that the system performs. Such issues include architecture, communications, allocation of functions, real-time processing, and distributed computing.

[2] Licensing aspects are discussed in Chapter 9.

in place to update the methods and the experience base as new digital I&C technologies and equipment are introduced in the future?

New Plants and Retrofits

Successfully dealing with the systems aspects of digital I&C applications is critically important to both new plant applications and retrofits. However, there are substantial differences between the two applications. For new plants, a large system is conceived and designed as such. The designers have relative freedom in configuring the system architecture and creating the various subsystems, which can be implemented on a plant-wide, fully integrated basis (see for example Figure 1-1 and companion description in Chapter 1). The size of the design task is usually matched by a large pool of available resources and the presence of a dedicated design team. Extensive testing of the subsystems and of the integrated system is also likely to be possible.

For retrofits or modifications, typically there will be a narrower focus and fewer resources available. The systems aspects of the particular application are likely to be relatively limited in scope, and in any case the designer is limited by the requirement of integrating the retrofit subsystem into an existing plant. For example, the designer will likely make more use of one-for-one digital-for-analog replacements. The customized nature of retrofits or modifications can make it difficult to carry out a series of changes in a consistent manner, unless there is an integrated, plant-wide plan.

Systems Aspects

The systems aspects of I&C systems in nuclear plants need to be considered from two perspectives: the plant (i.e., the nuclear, fluid, mechanical, and electrical systems) and the I&C systems themselves. More specifically, this includes:

- definition of the I&C systems, integration of these systems into the overall plant, and specification of the key high-level requirements applicable to all the I&C systems
- design of the individual I&C systems themselves, i.e., selection of design features intended to meet the high-level requirements

Interactively addressing the systems aspects from these two perspectives is essential in order for the design of the plant and the I&C systems to be adequately integrated, and to achieve (a) reliable plant operation, (b) reliable plant investment protection, and (c) reliable worker and public health protection. This is consistent with the normal design approach used to design such systems; see, for example, Johnson (1989) and Pradhan (1996). These authors discuss the design process in terms of the high-level function of problem definition, system requirements, and system partitioning. Once these steps are accomplished, the overall I&C system will be defined and divided into manageable systems or subsystems with defined top-level requirements.

The committee recognizes that individual digital systems are an important part of the successful implementation of large systems and that their design can be difficult. But there is a large body of experience, including numerous standards, with designing and successfully implementing these systems (see, for example, Center for Chemical Process Safety, 1995). There is also an extensive body of technical literature to guide this work. Therefore, the committee has focused on the higher-level aspects of digital I&C applications in nuclear power plants. It should be noted that there are several key areas in the design of digital systems that need to be carefully addressed, and these are summarized in Appendix F.

CURRENT U.S. NUCLEAR REGULATORY COMMISSION REGULATORY POSITIONS AND PLANS

In general, the U.S. Nuclear Regulatory Commission (USNRC) approach for addressing systems aspects is consistent with the above approach (looking at the I&C systems from two perspectives) and is generally described in Chapter 1 of this report. That is, high-level regulatory requirements are supplemented by more specific USNRC guidance and endorsements of industry standards. In discussion with the committee in October 1995, the USNRC staff called attention to top-level systems aspects requirements addressed in:

- 10 CFR 50.55a(h), endorsing the use of IEEE Standard 279–1971, particularly in paragraph 3, Design Basis, and paragraph 4.1, General Functional Requirement
- 10 CFR 50, Appendix A, Criterion 10, Reactor Design
- 10 CFR 50, Appendix A, Criterion 13, Instrumentation and Control
- 10 CFR 50, Appendix A, Criterion 20, Protection System Functions
- 10 CFR 50, Appendix A, Criterion 21, Protection System Reliability and Testability
- 10 CFR 50, Appendix A, Criterion 22, Protection System Independence
- 10 CFR 50, Appendix A, Criterion 23, Protection System Failure Modes
- 10 CFR 50, Appendix A, Criterion 24, Separation of Protection and Control Systems
- 10 CFR 50, Appendix A, Criterion 25, Protection System Requirements for Reactivity Control Malfunctions
- 10 CFR 50, Appendix A, Criterion 29, Protection Against Anticipated Operational Occurrences

In addition to these basic, high-level criteria, the USNRC staff noted that the existing review guidance includes:

- IEEE Standard 279–1971 and its alternate, IEEE Standard 603–1991
- IEEE 7-4.3.2–1993, in particular, Annexes E and F

The USNRC has recognized the need to revise and update their regulatory guidance documents to better address digital I&C systems, and it has an extensive revision under way (see Chapters 1 and 9). In the systems aspects area, the USNRC (1995) indicated the revision includes several items specifically directed at systems aspects. These include preparation of (a) a new branch technical position on digital systems architecture and real-time performance, which provides guidance on verifying limiting response times and architectural details; and (b) a new Standard Review Plan section, Section 7.9, Data Communications, which provides acceptance criteria and review guidance for data communications or multiplexers.

Applicability to Existing Plants

For existing plants the primary emphasis will be on digital upgrades and modifications. Thus, in addition to the documents listed above, the use of 10 CFR 50.59 will be very important. (See discussion in Chapter 1 and Chapter 9 regarding 10 CFR 50.59.)

Applicability to New Plants

There are three new plant designs being proposed by the U.S. nuclear industry, one from each of the major vendors, and these designs are being reviewed by the USNRC. All of these plant designs use I&C systems that are completely digital-based and fully integrated into the overall plant design. The USNRC review is being conducted under an alternative process set forth in 10 CFR 50.52. The basic technical requirements for licensing the plants are essentially the same as for existing plants, but the overall licensing review process defined in 10 CFR 50.52 is intended to be more streamlined and to result in the approval of standardized designs that can potentially be used at multiple sites.

An important part of the process of developing and documenting the design basis for these new plants has been the preparation and use of the Electric Power Research Institute's Utility Requirements Document (URD) (EPRI, 1992), which documents the requirements the utilities and vendors have agreed to impose on the new plant design. Chapter 10 (Man-Machine Interface Systems) of the URD sets forth requirements that specify the design approach for the digital I&C systems, requirements for the systems aspects, and requirements for specific systems.

To ensure the eventual licensability of the new plant design, the industry has sought formal review by the USNRC of the URD. The USNRC has reviewed the URD and has written formal Safety Evaluation Reports in which the USNRC agrees that a plant that meets the URD will likely meet the licensing requirements. USNRC review and acceptance of these requirements and their subsequent use in the design certification of the new plants has provided a way for the nuclear industry and the USNRC to reach agreement on many of the systems aspects of digital I&C. (See additional discussion of the URD in Chapter 1 above.)

DEVELOPMENTS IN THE U.S. NUCLEAR INDUSTRY

Existing I&C systems in U.S. nuclear plants are analog-based and are approaching or exceeding their life expectancy, resulting in increased maintenance efforts and costs to sustain system performance (see, e.g., a survey by Cross [1992] indicating that I&C maintenance costs are disproportionately high). As a result there is a strong interest in upgrading and modifying these systems. Many individual utilities are making upgrades, and an industry-wide initiative, led by the Electric Power Research Institute, is under way to promote cost-effective digital I&C upgrades (Chexal et al., 1991). The importance of systems aspects has been recognized in this initiative. For example, the EPRI initiative includes systems aspects in its retrofit implementation guidelines, which include guidance for defining equipment and interface requirements for plant data communications, architecture, systems requirements, and configuration management (see Machiels et al., 1995).

No new U.S. nuclear plants have begun construction in almost 20 years. As discussed above, however, three new nuclear plant designs have been proposed and are under review by the USNRC. All of these plants have fully digital-based I&C systems, and the specifications and other documents submitted for licensing review emphasize assuring that the design process and systems aspects are correctly defined so that the eventual detailed design and implementation will be successful. There is at least some indication that this approach is effective. An advanced nuclear power plant recently completed in Japan (Kashiwazaki-Kariwa unit 6) was started up with only very minor I&C system problems. This plant's design meets the bulk of the requirements for the equivalent U.S. advanced boiling-water reactor plant design being reviewed in the United States and, in fact, was used as a basis for developing many of the requirements contained in the Utility Requirements Document.

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

There have been several other nuclear plants completed in the last few years that use completely digital-based I&C systems and represent significant digital I&C integration efforts. These plants are in the United Kingdom (Sizewell-B plant), France (Chooz-B plant), Canada (Darlington plant), and Japan (Kashiwazaki-Kariwa unit 6). The committee has not reviewed these plant designs in detail. However, what is known about actual progress of the work on these plants and some of the problems that have occurred is instructive with respect to the importance of systems aspects of the design.

Sizewell-B includes a distributed digital control system for control and data acquisition, of a product family that has been extensively used in process control applications, including fossil fired generating stations. It also includes elements of a nuclear safety-grade product family for protection that has been used in some nuclear applications. Redundancy is provided at all levels, including the use of dual redundant conductors for data buses, and two diverse protection systems. Hard-wired controls and instruments provide backup for the computer-based systems (Boettcher, 1994).

Electricite de France (EDF) uses a three-level architecture for its N4 PWR series used at Chooz-B. One level is the digital protection system. Its mission is to bring the plant to a safe, stable status, maintaining core and containment integrity. A second level uses off-the-shelf hardware to provide functions such as boron control, pressure and temperature control, and monitoring of secondary feedwater supply. The third level is the human-machine interface in the control room, which includes hardwired controls connected directly to the lowest possible level of the I&C system (Nucleonics Week, 1995).

The Canadian nuclear program led the world in the use of digital technology. The CANDU reactors are physically large, and significant computations are required to maintain adequate neutron flux distribution and stability. As a result, digital systems have been extensively used in CANDU plants. Each new plant has had a greater scope of digital technology than the previous one. Darlington has digital systems in almost 100 percent of its control systems and over 70 percent of its plant protection system. Necessity and sound engineering have made digital I&C acceptable in the CANDU reactors (White, 1994).

As explained above, the Kawshiwazaki-Kariwa unit 6 in Japan meets the bulk of the requirements for the equivalent U.S. advanced boiling-water reactor plant design under review in the United States.

All of these plants are now producing power on the grid. Because the I&C systems are used extensively in the testing and startup phases as well as during operation at power, there are now several plant years of experience with these large systems. The implication of this experience is that such systems are clearly practical. Further, operation to date has been safe, although, as noted by Suri et al. (1995), large systems with long mission times are challenging tasks and may be subject to subtle failures that can take a long time to appear.

Three of the four plants have had systems aspects problems that were costly and caused delays. Sizewell-B and Chooz-B were affected by a problem that resulted in the need to both change the basic system design and change the control system suppliers in the middle of the design (Nucleonics Week, 1991). For the Darlington plant, a careful review of the software as part of the licensing process indicated that the software in its present form is satisfactory for use but will eventually need to be rewritten as changes inevitably arise (Joannou, 1995). The plant in Japan reported problems in a single part of the control system, but this was resolved in the startup program. On the basis of this experience it appears that systems aspects of nuclear plant I&C systems continue to warrant attention.

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

Safety-critical applications of digital I&C are widely used in the aerospace industry. Systems aspects have been the focus of many studies, particularly those addressing the role of the digital I&C systems in accidents and the lessons to be learned. Many of these deal with human-machine interfaces, task allocation, and levels of automation. One major finding closely related to systems aspects is the importance of operator confusion caused by automatic changes in operating modes (Aviation Week and Space Technology, 1995; IEEE Spectrum, 1995).

The chemical industry has great similarity to the nuclear industry in that it is a process industry that deals with (a) similar fluid conditions in terms of temperatures, pressures, and physical phase changes; (b) similar rotating machinery and mechanisms; and (c) significant latent energy storage, albeit of a different kind. Digital I&C systems have been extensively used in the chemical industry since the late 1970s. The industry has developed Guidelines for Safe Automation of Chemical Processes (Center for Chemical Process Safety, 1995), which contains details on important systems aspects, such as integrity of process control systems, process hazards, control strategies and schemes, safety considerations, data communications media, data reliability, and administrative considerations for system integrity.

DISCUSSION

During Phase 1 of its study, the committee recognized that a great many of the issues and problems being discussed and addressed in the nuclear industry were of a relatively specific nature that missed capturing the systems aspects of the application of digital I&C technologies. This preponderance of relatively specific issues is reflected in the discussions the committee chose to focus on in Chapters 4 through 8 below and in the many other candidate issues and topics considered by the committee (see Appendix D). Several members of the committee, however, had had personal experience in which the various specific parts of a system were apparently designed correctly but the ensemble or overall system did not perform satisfactorily. However, the committee feels that relatively specific I&C issues and problems are best addressed in the context of overall I&C system requirements and interfaces with the rest of the plant. For example, the committee was very much aware of the problems at the

Sizewell-B, Chooz-B, and Darlington plants, which were higher-level problems.

Sizewell-B and Chooz-B had to change their common original system supplier in the middle of the design efforts. The problem seems to have been the result of the underspecification of the Chooz-B system, and the complexity of the design. The original supplier found itself developing hardware and software in parallel to ever escalating requirements. Technical problems seem to have been created by the lack of adequate capacity to process the mass of acquired reactor data with the original architecture (Nucleonics Week, 1991). At Darlington, despite the high availability and safety record of the Canadian plants, the Canadian Atomic Energy Control Board undertook a more stringent review of the software engineering process and the operation of Darlington's first two units was delayed, with a resulting economic penalty on the utility.

The major lesson learned from these cases is that not only is the control of the design process important; equally important is the need for clear, complete, and stable requirements from the beginning of the project. To be clear, requirements must be quantified. Functions define what the system must do and must not do. Requirements define how well system functions must be performed.

The definition of clear, complete, and stable I&C requirements requires (a) an in-depth understanding of plant processes; (b) an in-depth understanding of the proposed I&C technology to be used; (c) the vision of what new features may be needed or desired in the new system, e.g., security, on-line maintenance aids; and (d) an ability to visualize and articulate the requirements in a top-down approach while keeping requirement conflicts out. The last component implies being able to look and see ahead for consistency as detailed "lower level" requirements are developed from the more global "top level requirements."

Finally, as noted above, the technical literature identifies the systems aspects of a design as being very important to achieving satisfactory performance, particularly as systems grow in size and complexity. There is thus a need to focus on the issue of systems aspects.

In dealing with systems aspects in U.S. nuclear power plants, there are some important factors to be taken into account: First, although three new U.S. plant designs are being reviewed by the USNRC, it is unlikely that any new nuclear plants will be built in the next few years in the United States. The U.S. plant experience will be limited to modifications or upgrades of limited scope, with the bulk of the upgrades and modifications involving component change-outs or small subsystems. Second, dealing with the systems aspects is not solely a USNRC responsibility. This is because systems aspects applies to both the safety and nonsafety systems and only a relatively small subset of the overall I&C systems in a nuclear plant fall under regulatory control. Industry must assure that systems aspects are properly dealt with for the nonsafety systems. The lessons learned and problems seen in foreign (nuclear) plants indicate nonsafety systems can cause problems. Note, for example, that the problems at Chooz-B and Sizewell-B occurred in the nonsafety portion of the plant (Nucleonics Week, 1995); nevertheless they were costly and should be avoided. Both the USNRC and the industry recognize that failures in the nonsafety systems can challenge the plant's design envelope and the safety systems must be appropriately designed to withstand these challenges and keep the plant within its safety envelope. Third, the existing U.S. nuclear plant I&C technology is largely analog-based. There is very little regulatory guidance regarding systems aspects for digital-based components. (As noted above, the USNRC has recognized this and has begun an upgrade of their requirements.)

Taking into account these realities of the situation in the United States, the committee discerned several activities that could be undertaken by the U.S. nuclear industry and the USNRC to better address systems aspects. The principle underlying these activities is that a proactive approach is appropriate for drawing on the available experience and expertise in other countries, comparable industries, and other government agencies. First, to assess whether new regulatory guidance documents have the needed specificity in the systems aspects area, a trial application could be made to the existing foreign plant experience that is already available and to new experience as additional foreign nuclear plants come on line. These new plants all use digital I&C technology throughout. These trial applications could be made both retrospectively to the existing plants and during development of new plants to see if the guidance is appropriate, effective, and of the desired specificity. Second, a systematic review could be made of the experience, techniques, and regulatory and industry guidance documents used in other comparable industries in the United States. Based on its own brief review, the committee has identified at least one candidate approach, one used in the chemical process industry, that merits consideration (Center for Chemical Process Safety, 1995). The committee expects that there are other likely sources of important experience and expertise, such as the aerospace industry, where large, fault-tolerant, safety-critical I&C systems are in wide use. For example, it would be useful for the USNRC to compare their new guidance documents with those available from the Federal Aviation Administration. Third, as digital systems continue to grow in power and complexity, and particularly in view of the probable lack of any new U.S. nuclear plants, action by the USNRC to maintain currency in systems aspects may also be warranted (Chapter 10 of this report discusses the general topic of technical infrastructure). Examples include:

- USNRC staff training and participation in key conferences in particularly germane technologies, such as fault-tolerant, distributed systems
- Participation by USNRC staff in the work of other domestic or foreign regulatory agencies (perhaps on a reciprocal loan basis) that are actively dealing with large-scale digital I&C systems

Finally, it is essential to pay careful attention to the specific design features of the individual I&C systems that are evaluated and licensed. Further, it is necessary to consider the details of the I&C system implementation and it is not sufficient to concentrate on general, high-level features. However, the committee's brief review of the applicable USNRC guidance found little specificity in these requirements regarding either level of the systems aspects, that is, the high-level systems aspects or the system design considerations covered in Appendix F. It appears that the USNRC should carefully consider the level of specificity provided in their regulatory guidance documents to be sure that the lessons learned from prior experience and in good design practice are adopted and followed. Appendix F is pertinent to this point.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. Continued effort is warranted by the USNRC and the nuclear industry to deal with the systems aspects of digital I&C in nuclear power plants.

Conclusion 2. The lack of actual design and implementation of large I&C systems for U.S. nuclear power plants makes it difficult to use learning from experience as a basis for improving how the nuclear industry and the USNRC deal with systems aspects.

Conclusion 3. The USNRC's intent to upgrade their regulatory guidance in the systems aspects of digital I&C applications in nuclear power plants is entirely supported by the committee's observations about systems aspects.

Conclusion 4. Existing regulatory guidance lacks the specificity needed to be effective, and the revision should address this shortcoming.

Recommendations

Recommendation 1. The USNRC should make a trial application of the proposed regulatory guidance documents on systems aspects to foreign nuclear plant digital systems, both existing and in progress. In particular, this review should focus on assessing whether or not the revised guidance documents have the necessary level of specificity to adequately address the systems aspects of nuclear plant digital I&C implementations.

Recommendation 2. The USNRC should identify and review systems aspects guidance documents provided in other industries, such as chemical processing and aerospace, where large-scale digital I&C systems are used. The focus of this review would be to compare these other guidance documents with those being developed by the USNRC, paying due attention to common problems and application-specific differences.

Recommendation 3. To obtain practical experience, the USNRC should loan staff personnel, perhaps on a reciprocal basis, to other agencies involved in regulating or overseeing large safety-critical digital I&C systems.

Recommendation 4. The USNRC should require continuing professional training for appropriate staff in technologies particularly germane to systems aspects, such as fault-tolerant, distributed systems.

REFERENCES

Aviation Week and Space Technology. 1995. Automated Cockpits: Who's in Charge? January 30 and February 6.

Boettcher, D. 1994. State-of-the-Art at Sizewell-B. Atom 433 (Mar–Apr):34–38.

Center for Chemical Process Safety. 1995. Guidelines for Safe Automation of Chemical Processes. New York: American Institute of Chemical Engineers.

Chexal, V., F. Lang, T. Marston, and K. Stahlkopf. 1991. An Industry Vision for the 1990s and Beyond. Nuclear Energy International 36(446):22–24, 26.

Cross, A.E. 1992. Analysis of corrective actions applied to nuclear power plant operations. Nuclear Safety 33(4): 586.

Electric Power Research Institute (EPRI). 1992. Advanced Light Water Reactor Utility Requirements Document. EPRI NP-6780-L, Vol. 2 (ALWR Evolutionary Plant) and Vol. 3 (ALWR Passive Plant), Ch. 10: Man-Machine Interface Systems. Palo Alto, Calif.: EPRI.

Institute of Electrical and Electronics Engineers (IEEE) Spectrum. 1995. The Glass Cockpit. September.

Joannou, P. 1995. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., December.

Johnson, B.W. 1989. Design and Analysis of Fault Tolerant Digital Systems. New York: Addison-Wesley.

Machiels, A., R. Torok, J. Naser, and D. Wilkinson. 1995. The Digital Challenge, An update on EPRI's I&C Upgrade Initiative. Nuclear Engineering International 40(489):44–46.

Nucleonics Week. 1991. British Support French I&C System That EDF Has Abandoned for its N4. January 10 and April 11.

Nucleonics Week. 1995. Outlook on I&C: Special Report to the Readers of Nucleonics Week, Inside the N.R.C. and Nuclear Fuel. September and October.

Pradhan, D.K. 1996. Fault-Tolerant Computer System Design. Upper Saddle River, N.J.: Prentice-Hall.

Suri, N., C.J. Walter, and M.M. Hugue. 1995. Advances in Ultra-Dependable Distributed Systems. Los Alamitos, Calif.: IEEE Computer Society Press.

U.S. Nuclear Regulatory Commission (USNRC). 1995. USNRC Staff (J. Wermeil) presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., October.

White, J. 1994. Comparative Assessments of Nuclear Instrumentation and Controls in the United States, Canada, Japan, Western Europe, and the Former Soviet Union. JTEC/WTEC Annual Report and Program Summary 1993/94. Baltimore, Md.: World Technology Evaluation Center, Loyola College.

4

Software Quality Assurance

INTRODUCTION

Software in nuclear power plants can be used to execute relatively simple combinational logic, such as that used for reactor trip functions, or more elaborate sequential logic, such as that used for actuating engineered safety features or for process control and monitoring. In either case, it must be ensured that required actions are taken and unnecessary trips are avoided.[1]

One way of assuring software quality is by examining and approving the process used to produce it. The assumption behind assessing the process by which software is produced is that high-quality software development processes will produce software products with similar qualities. An alternate approach to quality assurance is to directly evaluate properties of the software. Software properties include correctness, reliability, and safety.

Software is defined as correct if it behaves according to its requirements. Assurance of software correctness is sought either experimentally via program testing or analytically through formal verification techniques. Software may be correct but still not perform as intended, however, because of flaws in requirements (e.g., inconsistencies or incompleteness) or assurance techniques (e.g., failing to consider or design for all significant parts of the software's input space).

Software reliability is "the probability that a given program will operate correctly in a specified environment for a specified duration" (Goel and Bastani, 1985). Several models have been proposed for estimating software reliability (Musa et al., 1987).

Software is safe if it does not exhibit behaviors that contribute to a system hazard (i.e., a state that can lead to an accident given certain environmental conditions). Safety analysis and assurance techniques have been developed for all stages of the software life cycle (i.e., systems analysis, requirements, design, and code verification) (Leveson, 1995).

Complexity is an important aspect of assessing correctness, reliability, and safety of software. (The committee notes that complexity is of critical importance to the use of digital instrumentation and control [I&C] systems, and it is addressed in numerous places in this report.) For example, the committee is not aware of software metrics for complexity which are reliable and definitive.

Analog and digital systems should be analyzed differently because the assumptions underlying their design and production are different. Reliability estimation for analog systems primarily measures failures caused by parts wearing out, whereas for digital systems it seeks to address failures primarily caused by latent design flaws. Analog systems can be modeled using continuous and discrete functions, whereas digital systems must be modeled using discrete mathematics only. Although analog systems could contain similar latent design flaws, they are believed to be accommodated by existing evaluation techniques. When an analog system functions correctly on two "close" test points and continuous mathematics is applicable, it can be assumed that it will also function on all points between the two test points. This is not necessarily true for digital systems, which may produce very different results for similar test points.

Statement of the Issue

The use of software is a principal difference between digital and analog I&C systems. Quality of software is measured

[1] Although this chapter covers *software* quality assurance, its conclusions apply to any technology requiring equivalent design effort, e.g., field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), and programmable logic controllers (PLCs). Digital hardware designs can range in complexity from a simple circuit to a microprocessor to a general purpose computer. The complexity of a design is not eliminated or changed simply by expressing the design in a different form. The committee has seen no proof that software that is implemented on an ASIC is unlikely to have a different level of reliability or to be more verifiable. Testability (which is related to complexity) is not changed simply because the form of the software instructions has changed from a set of programming language instructions to a set of gate arrays. However, software implemented in ASICs (as well as software stored in read-only memory) does have configuration control advantages in that unintended changes to the software outside the configuration management system becomes much more difficult.

in terms of its ability to perform its intended functions. This, in turn, is traced to software specifications and compliance with these specifications. Neither of the classic approaches of (a) controlling the software development process or (b) verifying the end-product appears to be fully satisfactory in assuring adequate quality of software, particularly for use with safety-critical systems. How can the U.S. Nuclear Regulatory Commission (USNRC) and the nuclear industry define a generally accepted, technically sound solution to specifying, producing, and controlling software needed in digital I&C systems?

Discussion

High quality software results from the use of good software engineering practices during development to minimize the probability of introducing errors into the software, and a rigorous verification process to maximize the probability of detecting errors. Good software engineering practices (e.g., structured programming and data abstraction) reduce the amount of information that developers must remember when writing, analyzing, or changing software. However, good software engineering methods are not easy to apply, and the methods only reduce rather than eliminate errors (Parnas, 1985). Thus software verification activities remain a key concern.

Software verification seeks to determine that the software being built corresponds to its specification, and software validation seeks to demonstrate that the system meets its operational goals. Verification and validation (V&V) activities may focus on either the process or the product. Process-oriented V&V focuses on the process by which the software is produced. It typically involves performing and observing inspections and evaluating test results. Product-oriented V&V focuses on testing and evaluating the final product, independent of the process.

Different techniques for assessing software quality have been developed. These techniques fall into two broad categories, analytic or experimental, each of which encompasses a large number of methods. Analytic techniques include inspections or walk-throughs and formal analysis methods based on mathematics. Program testing is the most common experimental analysis technique.

In software reviews or inspections, teams of software developers examine software artifacts for defects. Participants may be given lists of questions about the artifact that they must answer in order to ensure that they are sufficiently prepared for an inspection, and they may be given lists of potential errors for which they are to check. Inspections have proved to be an effective method for detecting software defects (Fagan, 1976). Requirements inspections catch errors before they propagate into designs and implementations, making them less costly to repair. Also, inspections subject a software artifact to the scrutiny of several people, some of whom would not have participated in the artifact's design. Successful inspections depend on the experience levels of the participants and the quality of the artifacts inspected (Porter et al., 1996). They also depend on the requirements being expressed in a precise, unambiguous manner so the reviewers are able to check the document without having to make assumptions on how the system will be implemented. This can be challenging in practice because it is difficult to find a notation such that reviewers are able to effectively check the correctness of the requirements rather than focusing on the details of the notation. Furthermore, the notation must be "readable" by both users and developers.

Formal methods[2] use mathematical techniques to assess if an artifact is consistent with a more abstract description of its general and specific properties (Rushby, 1993). General properties derive from the form of the artifact's description (e.g., that functions are total, that axioms are consistent, or that variables are initialized before they are referenced). Specific properties derive from the problem domain and are captured in an abstract description. Verification using formal methods involves the comparison of a more detailed description of a software system with the more abstract description of its properties. Verifying specific properties of programs using formal methods has proved to be very difficult (Gerhart and Yelowitz, 1976; Rushby and von Henke, 1991, 1993). Furthermore, making mathematical proofs does not guarantee the software will function correctly. Even if one could perform the verification using formal methods, testing would still be necessary to validate the assumptions in the proofs. These assumptions would include that the model matches the real world and that the code statements will behave as modeled when executed on the target hardware. Moreover, errors are often made in proofs.

Testing is used to expose program flaws and to estimate software reliability. Black-box testing seeks to determine if software has functional behavior that is consistent with its requirements. Black-box testing is concerned only with inputs and outputs. White-box testing addresses the internal structure of software (e.g., the outcome of its logical tests) and seeks to exercise the internal structure:

> Some engineers believe one can design black box tests without knowledge of what is inside the box. This is, unfortunately, not completely true. If we know that the contents of a black box exhibit linear behavior, the number of tests needed to make sure it would function as specified could be quite small. If we know that the function can be described by a polynomial of order 'N,' we can use that information to determine how many tests are needed. If the function can have a large number of discontinuities, far more tests are needed. That is why a shift from analogue technology to software brings with it a need for much more testing (Parnas et al., 1990).

[2] The committee does not make a blanket endorsement of "formal methods." However, the committee considers that elements of formal methods are useful and appropriate and has indicated in the report specific instances where they should be used. For example, see Recommendation 2 in this chapter.

In testing, practitioners seek to find suitable test cases so that if the software exhibits acceptable behavior for these cases it can be inferred that it will work similarly for other cases. However, complex software systems have large numbers of states and irregular structure. Testing can only sample a fraction of these states, and it cannot be inferred that untested states are free from errors if none are exhibited in tested states. As Dijkstra (1970) points out, "Program testing can be used to show the presence of bugs, but never to show their absence!"

Software standards can help achieve acceptable levels of software quality. Because software development practices are constantly improving, standards should not require developers to use particular techniques. However, standards can include definitive acceptance criteria. An example of definitive and objective acceptance criteria in existing standards is the requirement for white-box structural coverage in the Federal Aviation Administration standard, Software Considerations in Airborne Systems and Equipment Certification (DO-178B). Depending on the safety category, software logic must be test-exercised until the specified acceptance criteria have been met.

There are several existing standards for the production of safety-critical software for nuclear power plants. These include IEC 880, Software for Computers in the Safety Systems of Nuclear Power Stations (IEC, 1986) and IEEE 7-4.3.2–1993, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (IEEE, 1993). IEC 880 outlines the software development techniques to be used in the development of software for the shutdown systems of nuclear power plants. Rather than mandate particular techniques, IEC 880 states the requirements on the product; it is up to the developer to meet those requirements using whatever techniques the developer considers suitable. There are guidelines presented in an appendix to IEC 880 that describe the effects that particular techniques are expected to achieve.

IEEE 7-4.3.2–1993 advocates choosing a combination of the following V&V activities: independent reviews, independent witnessing, inspection, analysis, and testing. Some of these activities may be performed by developers, but independent reviews must subsequently be performed. Walk-throughs of design, code, and test results are recommended inspection techniques. Analysis includes, but is not limited to, formal proofs, Petri net and other graphical analysis methods, and related techniques. Functional and structural testing are recommended for any software artifact that is executable or compilable. Testing of nonsafety functions may be required to provide adequate confidence that nonsafety failures do not adversely impact safety functions. The standard points out that functional testing cannot be used to conclusively determine that there are no internal characteristics of the code that would cause unintended behavior unless all combinations of inputs, both valid and invalid, are exhaustively tested.

IEEE standards have been criticized as "ad hoc and unintegrated" because they have been developed in a piecewise fashion (Moore and Rada, 1996). Generally, IEEE 7-4.3.2–1993 does not suggest which V&V activities are most effective, nor does it discriminate between activities that are mainly actuarial (e.g., witnessing) and those that are technical (e.g., analysis and testing). In addition, the standard states that path testing is feasible. Except for extremely simple programs, however, numerous references have shown that path testing requires an infeasible number of tests (e.g., Myers, 1979). Therefore, for most practical programs, path testing is infeasible. Furthermore, even if path testing were feasible and were performed, the resulting program could still have undetected errors: for example, there could be missing paths, the program might not satisfy its requirements (the wrong program could have been written), and there could be data-sensitivity errors. (As an example of a data-sensitivity error, suppose a program has to compare two numbers for convergence, that is, see if the difference between two numbers is less than some predetermined value. One could write: "If $A - B < \varepsilon$ then…" But this is wrong, because the comparison should have been with the absolute value of $A - B$. Detection of this error is dependent on the values used for A and B and would not necessarily be found by simply executing every path through the program.)

Once high-quality software has been prepared initially, it is likely to undergo continuous change to accommodate new hardware, fix latent errors, or add new functions to existing systems. Configuration control requires rigorous review and formal approval of software changes. Managing multiple versions of software systems and assuring that changes do not degrade system reliability and safety is a difficult problem.

CURRENT U.S. NUCLEAR REGULATORY COMMISSION REGULATORY POSITIONS AND PLANS

Current Positions

The USNRC regulatory basis for software quality assurance is given in:

- 10 CFR 50.55a(h), Protection Systems, which mandates the use of IEEE Standard 279–1971, Criteria for Protection of Systems for Nuclear Power Generating Stations
- Title 10 CFR Part 50, Appendix A, General Design Criteria for Nuclear Power Plants (Criterion 1, Quality Standards and Records; Criterion 21, Protection System Reliability and Testability; Criterion 22, Protection System Independence; and Criterion 29, Protection Against Anticipated Operational Occurrences)
- Title 10 CFR Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing

Plants (Section III, Design Control; Section V, Instructions, Procedures, and Drawings; and Section VI, Document Control)

To provide more specific guidance, the USNRC uses Regulatory Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants, and ANSI/IEEE/ANS 7-4.3.2–1982, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations (promulgated jointly by the American National Standards Institute, the Institute of Electrical and Electronics Engineers, and the American Nuclear Society), in conducting software reviews. Other standards are used as reference, e.g., IEEE 1012–1986, IEEE Standard for Software Verification and Validation Plans, and ASME [American Society of Mechanical Engineers] NQA-2A–1990, Part 2.7, Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications. The Standard Review Plan cites and makes use of these standards and is an attempt to integrate their various requirements.

Staff Reviews

USNRC staff reviews of the V&V processes used during software development seem quite thorough. One particularly good example is the staff review of the V&V process for the Eagle 21 reactor protection system installed at Zion Units 1 and 2 (USNRC, 1992). Staff activities included comparing V&V to ANSI/IEEE/ANS 7-4.3.2–1982, verifying the independence of V&V personnel, reviewing the development of functional requirements and subsequent software development documents, and reviewing software problem reports and fixes. They also performed a thread audit by picking sample plant parameters and tracing the software development from developing the requirements to the writing and testing of code. This review included reviewing code on a sample basis, comparing software development documents and code, and examining software problem reports and corrections. The entire system was also examined for potential timing problems between the software and hardware.

The staff noted: “Experience with computer projects has demonstrated that the development of computer system functional requirements can have a significant impact on the quality and safety of the implemented system” (USNRC, 1992). The staff randomly sampled 56 of the 408 problem reports and found that 21 percent had significant implications (e.g., equations that did not match requirements or logic defects). Discovery of this type of error raised the staff’s concerns regarding the potential for common-mode failures in digital electronics and convinced the staff that rigorous V&V activities were needed to augment the developer’s functional tests. The staff’s thread audit discovered three discrepancies between the requirements and the design documents (e.g., a piece of source code that the requirements seemed to mandate but that was omitted in the design). The staff concluded that although there were problems in implementation of the V&V plan, the basic plan was sound. The staff also considered whether the use of different releases of compilers affected the correctness of the software. They also considered Commonwealth Edison’s configuration management program for the software. The USNRC approved the approach taken on both of these issues.

Research and Plans

The seven existing sections of Chapter 7 of the 1981–1982 version of the Standard Review Plan (SRP) are being updated (project completion expected in June 1997) to incorporate digital technology aspects. Two new sections are being added (Section 7.8, Diverse I&C Systems, to deal with the ATWS [anticipated transients without scram] rule and the defense-in-depth and diversity analysis of digital safety I&C systems, and Section 7.9, Data Communications, to deal with new issues like multiplexing). New branch technical positions are also being developed for inclusion in the SRP update, including ones on software development process, software development outputs, and programmable logic controllers.

As part of the SRP update process, the USNRC is developing regulatory guides to endorse (with possible exceptions) 10 industry software standards:

- IEEE 7-4.3.2–1993, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (an update of the 1982 version)
- IEEE 603–1991, Standard Criteria for Safety Systems in Nuclear Power Generating Stations (follow-on to IEEE 279–1971)
- IEEE 828–1990, Standard for Configuration Management Plans
- IEEE 829–1983, Standard for Software Test Documentation
- IEEE 830–1984, Guide for Software Requirements Specifications
- IEEE 1008–1987, Standard for Software Unit Testing
- IEEE 1012–1986, Standard for Software Verification and Validation Plans
- IEEE 1028–1988, Standard for Software Reviews and Audits
- IEEE 1042–1987, Guide to Software Configuration Management
- IEEE 1074–1991, Standard for Developing Life Cycle Processes

The USNRC also has ongoing research programs. One of these, called Review and Assessment of Software Languages for Use in Nuclear Power Plant Safety Systems, is assessing advantages and disadvantages of programming languages used in safety systems. Another, called Measurement Based Dependability Analysis for Digital Systems, is analyzing operational failure data to estimate failure probabilities.

Finally, as a member of the Halden Reactor Project, the USNRC is following research being conducted at the project on the use of formal methods in development and in quality assurance/licensing issues.

DEVELOPMENTS IN THE U.S. NUCLEAR INDUSTRY

Vendors

During the course of Phase 2 activities, the committee talked with three digital I&C vendors about software quality assurance: Foxboro Controls, General Electric Nuclear Engineering, and Westinghouse. Vendors reported developing systems containing at least 10,000 lines of code in a mixture of high-level and assembly languages. Their software quality assurance programs were generally modeled after IEEE 7-4.3.2–1993 and IEC 880 and had been audited and approved by USNRC staff.

Nuclear Utilities

In Phase 2, the committee also talked with a number of nuclear utilities engaged in digital I&C upgrades: Baltimore Gas and Electric Company, Public Service Electric and Gas (PSE&G) Company, Northeast Utilities, and Pacific Gas and Electric Company. Representatives from several of the utilities mentioned that strong requirements analysis and configuration control were keys to producing high-quality software. The representatives noted that strong analysis requirements and configuration control should be applied to safety-critical software *and* nonsafety software, even though nuclear plant designs routinely separate the hardware and software so that nonsafety software does not run on the same computer as the safety-critical applications. It is clear that high standards must be applied to software running on safety-critical computers since any such program has the potential to cause a safety-critical failure. The utility representatives emphasized that the same strong requirements should be applied to the nonsafety software because even nonsafety applications could malfunction in such a way that safety systems could be required to respond and have safety implications. They also noted that hazard/failure analyses should be part of a V&V program. PSE&G described a four-stage review that considers hardware-software interactions, the software development process, thread analysis of a small number of functions, and component-based failure analysis.

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

During the course of Phase 2 activities, the committee also talked with representatives from the Canadian and Japanese nuclear power industry and had access to information on the British experience with digital I&C systems pertaining to software quality assurance. A representative from Mitsubishi Heavy Industries asserted that they rely on the IEC 880 standard for software quality assurance. British Nuclear Electric issued Nuclear Electric Programmable Electronic Systems guidelines for the quality assurance of digital I&C systems.

Considerable controversy surrounds the results of British Nuclear Electric's tests of the Sizewell B primary protection system (PPS). These tests were not part of system validation testing, but rather a set of tests concentrated on infrequent fault scenarios that were designed to support safety claims made for the PPS (W.D. Ghrist III, personal communication to the committee, May 1996). Most test results were to be resolved automatically by use of a test driver that compared them to responses predicted from a model, and the remainder were to be resolved manually. However, only half of the first 50,000 tests were resolved automatically, resulting in reports that the PPS failed 50 percent of its tests. Manual inspections of test results were necessary because of timing problems between the PPS and the test driver. For example, inputs were not being provided to the PPS fast enough to prevent it from indicating failures of incoming data link communications, or the PPS responded at a rate much faster than input values were changing. In fact, only three or four errors were found in time delay and setpoint levels because of specification discrepancies.

One conclusion that could be drawn about this experience is that there were problems with the completeness and configuration control of the requirements: Understanding the response time of the PPS required knowledge of the system design as well as the requirements; hysteresis information was in the original functional specification but not the specification provided to the test group; and default actions on some input quantities were omitted from the specifications.

Canada's Atomic Energy Control Board (AECB) licensed a computerized shutdown system at Atomic Energy of Canada Limited's (AECL) Darlington plant operated by Ontario Hydro. The AECB had originally raised objections about the lack of a widely accepted definition of what constituted "good enough" for safety-critical software. Ontario Hydro used formal methods to verify the consistency of the software and the requirements and also used tests randomly chosen to model one of six accident scenarios to demonstrate the system's reliability (Joannou, 1993).

Ontario Hydro and AECL embarked on an effort to develop standards for the software engineering process, the outputs from the process, and the requirements to be met by each output. The standards, called OASES, use a graded approach based on categories of criticality. For each category, OASES defines a software engineering process, procedures used to perform activities within each step of a process, and guidelines defining how to qualify already developed software in each category. OASES is a more unified approach to developing standards than the USNRC approach of developing standards for individual process activities.

The AECB has also developed a draft regulatory guide, C-138, Software in Protection and Control Systems, for software assessment (AECB, 1996). They stress that "evidence of software completeness, correctness, and safety will have to be reviewed and understood by people other than those who prepared it." Several aspects were identified as critical for providing evidence of high-quality software:

- software requirements specification
- systematic inspection of software design and implementation
- software testing
- the software development process and its management

The AECB draft regulatory guide (AECB, 1996) includes a number of acceptance criteria:

- Software requirements should be unambiguous, consistent, and complete. Requirements should be precise enough to distinguish between correct and incorrect implementations, and mechanical rules should exist for resolving disputes about the meanings of requirements. The attributes indicate that a formal notation be used. The notation should define how continuous quantities in the environment can be represented by discrete values in software.
- Systematic inspections should include functional analysis to provide evidence that the software does what it is defined to do, and software safety analysis to provide evidence that the software does not initiate unsafe actions. Functional analysis should be based on formally defined notations and techniques so that mathematical models and automated tools can be used. A system-level hazard analysis should determine the contribution of software to each hazard, and analysis should extend into the software to increase confidence that hazardous states cannot occur.
- Both functional and random testing should be employed. Functional tests should be chosen to expose errors in normal and boundary cases, and measures of test coverage should be reported for them. Random tests selected from input conditions should be used to demonstrate that the software will function without failure under specific conditions.
- Software design and implementation methods are rapidly improving. Instead of mandating a single set of methods, the guide specifies that software be developed "by properly qualified people following a controlled and accepted software development and quality assurance plan." Methods selected should enable software designs and implementations to be reviewed to determine if quality attributes (e.g., completeness, consistency, etc.) have been attained.
- Configuration management should be used to control change. Changes should be justified and reviewed, and all artifacts (e.g., designs and test plans) relating to the component being changed should also be updated. Changed release versions (with indicated changes) should be distributed to all holders of the original versions, including the regulatory agency.

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

During the course of Phase 2 activities (see Appendix B), the committee heard presentations from John Rushby of SRI International, committee member Michael DeWalt of the Federal Aviation Administration, Joseph Profetta of Union Switch and Signal Inc., and Lynn Elliott of Guidant Cardiac Pacemakers. The committee also examined the circumstances surrounding problems in other applications.

Dr. Rushby summarized his experience with a number of high-assurance software systems by stating that mishaps are generally due to requirements errors rather than coding errors. Current techniques for quality assurance are adequate for later software development stages (e.g., coding). However, early stages have weak V&V methods because of a lack of adequate validation techniques, particularly for systems with complex interactions (e.g., concurrent, fault-tolerant, reactive, real-time systems). Dr. Rushby suggested that formal methods could be used to specify assumptions about the environment in which a system operates, the requirements of the system, and a design to accomplish the requirements. If these specifications were written, they could be analyzed for certain forms of consistency and completeness and validated by posing "challenges" as to whether a specification satisfies a requirement or whether a design implements a specification.

Committee member DeWalt presented the FAA's Software Considerations in Airborne Systems and Equipment Certification (DO-178B), which provides guidelines for the production of software for airborne systems. These guidelines represent an industry and regulator consensus document. The guidelines used by the FAA identify 66 objectives covering the entire software development process. These objectives represent a distillation of best industry practices and do not rely on or reference other standards or guidelines. The number of objectives that must be satisfied and the associated rigor applied is a function of five different severity categories of safety. These objectives for the most part have objective acceptance criteria understood by the regulators and industry. The compliance of a specific software product with the guidelines is established by examining data products produced by the software process and interviewing developer personnel. The guidelines recognize that objectives can be satisfied by alternative methods (e.g., service experience) provided that equivalent levels of confidence can be demonstrated. The FAA also has a delegation system that allows industry representatives to make compliance findings on behalf of the FAA.

Mr. Profetta described the distributed process control systems in which control signals from remote controllers could be overridden by local signals in trains or switches. Critical software is developed following IEEE standards and development processes. Quality is assured via extensive testing on a simulation of a train control system. The application has very well-defined safety problems, and only six events are needed to characterize the problems. Extensive testing is undertaken using seeded faults to estimate the probability that test cases expose faults.

Mr. Elliott stated that his most difficult software development problem was writing and reviewing requirements specifications. Food and Drug Administration (FDA) regulators expect natural language requirements, but Mr. Elliott has found that describing systems with Statemate (Harel et al., 1990), a notation for describing event-driven reactive systems, is superior to either natural language or data flow diagrams. Guidant Cardiac Pacemakers developers use fault tree analysis to analyze the safety of their system and dynamic testing to ensure the software's behavior. FDA regulators specify guidelines for these activities but do not prescribe particular development methods.

A prior NRC study of space shuttle avionics software (NRC, 1993) identified shortcomings of inspections with respect to assumptions reviewers made about hardware and software platforms on which their implementations execute. Inspections focus on the development of software by a single contractor, and do not probe beyond the descriptions of interfaces supplied by other contractors. As a result, implementations are vulnerable to errors arising from assumptions made about erroneously documented interfaces.

The Ariane 5 failure (Lions et al., 1996) offers a cautionary note for drawing conclusions about the reliability or safety of software based on prior operating experience. The first flight of the Ariane 5 launcher ended in a failure caused by responses to erroneous flight data provided by alignment software in its Inertial Reference System. Part of the data contained a diagnostic bit pattern which was erroneously interpreted as flight data. The alignment software computes meaningful results only before lift-off. After lift-off, this software serves no purpose.

The original requirement for the continued operation of the alignment software after lift-off was retained during 10 years of the earlier models of Ariane, in order to cope with a hold in the countdown. The period selected for continued alignment operation was based on the time needed for the ground equipment to resume full control of the launcher in the event of a hold.

The same requirement does not apply to Ariane 5, but was maintained for commonality reasons, presumably based on the view that, unless proven necessary, it was not wise to make changes in software which worked well on Ariane 4.

REVIEW OF EXPERIENCE

In order to better understand what types of software problems have occurred in software quality assurance, the committee reviewed a number of licensee event reports (LERs, which are submitted to the USNRC) and summaries of LERs reporting problems with computer-based systems in nuclear power plants. LERs describing events at Diablo Canyon (LER 92-028-00), Salem (LER 92-107-00), and Turkey Point (LER 94-005-02) identify instances of software design errors, inadequate review of requirements and designs, excessive reliance on testing as a V&V method, and problems with configuration control. The Turkey Point incident illustrates several problems that can occur.[3]

The Florida Power and Light (FPL) Company's Turkey Point LER describes an upgrade to the Turkey Point Unit 3 and 4 emergency power system (EPS) using commercial-grade programmable logic controllers (PLCs) in the EPS load sequencer. FPL stated that these new load sequencers would replicate the functions of the old sequencers, with some improvements to the sequence timing for loading of safety equipment. In response to USNRC review, FPL committed to follow the verification and validation program in IEEE 1012–1986, Standard for Software Verification and Validation Plans, and the guidelines in Regulatory Guide 1.152, which endorses ANSI/IEEE/ANS 7-4.3.2–1982, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations. Additionally, the contractor responsible for developing and installing the load sequencer performed independent V&V of the PLCs and the load sequencer logic.

FPL qualified the PLCs as Class 1E through dedication of the commercial-grade equipment based on guidance provided in EPRI [Electric Power Research Institute] NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications. FPL guaranteed that all logic functions would be tested under the guidelines of the above-mentioned V&V program, particularly to ensure that there were no common-mode failures between the redundant trains of load sequencers. FPL stated that in addition to the regularly scheduled startup and bus load tests, the load sequencer would be tested "continuously" using an automatic self-test mode. This enhancement was approved by the USNRC (Newberry, 1990).

On November 3, 1994, Turkey Point Unit 3's sequencer failed to respond to Unit 4's safety injection (SI) signal because of a defect in the sequencer software logic. The defect could inhibit any or all of the four sequencers from responding to input signals. The problem arose in trying to design the sequencers so that if a "real" emergency signal is received while the sequencer is being tested, the test signal clears and the engineering safety features controlled by the sequencer are activated.

As actually implemented, if an SI signal is received 15 seconds or later into particular test scenarios, the test signal is cleared but the inhibit signal preventing actuation is

[3] The Diablo Canyon plant is in Avila Beach, California; the Salem plant is in Salem, New Jersey; the Turkey Point plant is in Florida City, Florida.

maintained by latching logic. The test signal initiates the latching logic, but an input signal maintains the latching logic if the signal arrives prior to the removal of the test signal. Thus, if a real signal arrives more than 15 seconds into the test scenario, the test signal clears but the inhibit logic is held locked in and actuation is prevented. As the result of erroneous inhibit signals, any sequencer output might be blocked. The outputs blocked are determined by a combination of factors, including which test scenario was executing, the length of time the test was running, and which other inputs were received.

The designer and independent verifier failed to recognize the interactions between the inhibit and test logic. An independent assessment team found that logic diagrams contained information not reflected in the ladder diagrams, and that the V&V was not comprehensive enough to test certain aspects of the logic. In its review, the USNRC stated, "The plan was weak in that it relied almost completely on testing as the V&V methodology. More emphasis on the analysis of the requirements and design would have increased the likelihood of discovering the design flaw." This incident illustrates many of the potential problems with digital systems: added design complexity from self-testing software components, incomplete requirements, and inadequate testing.

Two recent studies by Lee (1994) and Ragheb (1996) provide data on digital application experiences in the United States and Canada. Lee reviewed 79 LERs for digital failures and classified them according to their root causes. With respect to the U.S. experience, Lee found that electromagnetic interference (EMI), human-machine interface error, and software error caused a "significant number of failures" (where "significant" is not defined in the report) in digital components during the three-year period studied (1990–1993). Fewer digital system failures involved random component failure. The actual numbers are shown in Table 4-1. The report concludes that the root causes of these failures were (1) poor software V&V, (2) inadequate plant procedures, and (3) inadequate electromagnetic compatibility of the digital system for its environment.[4]

TABLE 4-1 U.S. Software-Related LERs between 1990 and 1993

Cause of Events	Number of Events
Software error	30
Human-machine interface error	25
Electromagnetic interference	15
Random component failure	9

Source: Lee (1994).

Although the study is not yet completed, the Canadian AECB has been reviewing data from the United States, Canada, and France on software failures in nuclear power plants (Ragheb, 1996). The reviews include only events that resulted in consequences that meet reporting criteria of the government agency and do not necessarily include all digital system failures. The results of this study are in draft form only and may change before final publication. It is also important to note again that classification of errors is very difficult and may be subject to the classifier's biases or personal definitions.

In the AECB study, 459 event reports from 22 reactors over 13 years are being evaluated. The AECB found all trends either decreasing or flat, except those attributable to inappropriate human actions (which have shown a marked increase in the last five years). Hardware problems overall were found to be decreasing with time, although peaks can be found in some recent years. The number of software faults appears to be relatively constant over time.[5]

A large majority of the computer-related events occurred in digital control systems, which is not surprising given that they have been in operation the longest (since 1970) and perform a complex and continuous task: 363 computer system failures were in control systems, 29 in shutdown systems, and 65 in other systems. Table 4-2 shows the distribution of the failure types.

Of the problems classified as relating to software, 104 involved application software, four involved the executive or operating system, four a database or table, and five were classified as other.

We emphasize that the classification of the errors in this report was subjective and thus the data should be used with caution. However, it does appear that a number of software errors have been found in operating nuclear power plant software and more extensive evaluation and collection of data would be useful in making decisions about most of the issues in this report.

Finally, Ragheb notes that introducing modern digital I&C systems may not alleviate software quality assurance concerns. He points out: "Programmable logic controllers (PLCs) are being introduced as a cost-effective method of replacing older analogue or digital controls. PLCs have resulted in a number of incidents within the plants and it must be recognized that they are themselves digital computers."

A study of PLCs used in a U.S. phenol plant (Paula, 1993) reported a processor failure rate of approximately two per

[4] Experience shows that classification of incidents into categories solely using LER data is fraught with uncertainty and likely to be erroneous because of the great difficulty of determining root causes from the summary data in the LERs. Further, committee review of Lee's classification indicates several questionable or apparently erroneous classifications. Nevertheless, the committee agrees that inadequate V&V is a substantial problem that must be addressed.

[5] Ragheb was also critical of temporary software modifications performed by "patching" the software to change its behavior. For example, at the Canadian Bruce-A plant, the software was patched to permit the software to operate correctly at very low reactor power. However, the patch was not removed when the reactor power increased, and "the software operated incorrectly and caused a power excursion that was terminated by a trip" (Ragheb, 1996).

TABLE 4-2 Summary of Canadian Software-Related Event Reports 1980–1993

Failure Cause	Number
Software problems	117
Human-machine interface problems	130
Hardware problems	220
External (power, electromagnetic interference, other)	39
Unassigned	37

NOTE: Total number of failure causes exceeds number of events. Some events apparently had multiple causes.

Source: Ragheb (1996).

year. The plant operators also reported a total of our complete PLC failures (both primary and secondary processors) for all PLCs over seven years of plant operation. No PLC failures were reported because of errors in the software, including operating systems and applications software, or because of operator error. For PLCs with fault-tolerant redundant architectures installed to perform control interlocks in several nuclear power plants of French design, Paula found there were 58 failures of both processors out of a total 1,200 PLCs over a three-year period (Paula, 1993).

In evaluating these data, Paula warns that system size and complexity are important factors. The PLCs considered are relatively simple, generally accepting a few input signals and performing only a few control functions. In a study of fault-tolerant digital control systems that are much larger and more complex than these PLCs, the failure rates were about 15 to 50 times higher (Paula et al., 1993). In these fault-tolerant digital control systems, software errors were an important contributor to system failure. In several of the systems studied, failure due to software errors occurred as often as hardware failures, and the authors further (Paula et al., 1993) conclude that software errors tended to be difficult to prevent because they may occur only when an unusual set of inputs exists. Inadvertent operator actions, particularly during maintenance, also contributed significantly to the frequency of failures of these fault-tolerant digital control systems.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. Software quality assurance procedures typically monitor process compliance rather than product quality. In particular, there are no generally accepted evaluation criteria for safety-related software; rather, standards and guidelines help to repeat best practices. Because most software qualities related to system safety, e.g., maintainability, correctness, and security, cannot be measured directly, it must be assumed that a relationship exists between measurable variables and the qualities to be ensured. To deal with this limitation, care must be taken to validate such models, e.g., using past development activities, and to assure that the measurements being made are appropriate and accurate in assessing the desired software qualities.

Conclusion 2. Prior operating experience with particular software does not necessarily ensure reliability or safety properties in a new application. Additional reviews, analysis, or testing by a utility or third-party dedicator may be necessary to reach an adequate level of assurance.

Conclusion 3. Testing must not be the sole quality assurance technique. In general, it is not feasible to assure software correctness through exhaustive testing for most real, practical I&C systems.

Conclusion 4. USNRC staff reviews of the verification and validation process used during software development seem quite thorough.

Conclusion 5. Exposing software flaws, demonstrating reliable behavior of software, and finding unintended functionality and flaws in requirements are different concepts and should be assessed by a combination of techniques including:

- Systematic inspections of software and planned testing with representative inputs from different parts of the systems domain can help determine if flaws exist in the software.
- Functional tests can be chosen to expose errors in normal and boundary cases, and measures of test coverage can be reported for them.
- Testing based on large numbers of inputs randomly selected from the operational profiles of a program can be used to assess the likelihood that software will fail under specific operating conditions.
- Requirements inspections can be an effective method for detecting software defects, provided requirements are studied by several experienced people who did not participate in their construction. The effectiveness of these reviews also depends on the quality of the requirements.
- A system-level hazard analysis can identify states that, combined with environmental conditions, can lead to accidents. The analysis should extend into software components to ensure that software does not contribute to system hazards.

Conclusion 6. The USNRC research programs related to software quality assurance appear to be skewed toward investigating code-level issues, e.g., coding in different languages to achieve diversity and program slicing to identify threads containing common code.

Conclusion 7. Rigorous configuration management must be used to assure that changes are correctly designed and implemented and that relationships between different software artifacts are maintained.

Conclusion 8. Software is not more testable simply because the design has been implemented on a chip. Use of any technology requiring equivalent design effort to software requires commensurate quality assurance. For example, this conclusion applies to ASIC (application-specific integrated circuit), PLC (programmable logic controllers), and FPGA (field programmable gate arrays). However, the committee notes that the use of these technologies may be useful in addressing some configuration management problems.

Recommendations

Recommendation 1. Currently, the USNRC's path is to develop regulatory guides to endorse (with possible exceptions) a variety of industry standards. The USNRC should develop its own guidelines for software quality assurance that focus on acceptance criteria rather than prescriptive solutions. The draft regulatory guide, Software in Protection and Control Systems, by Canada's Atomic Energy Control Board is an example of this type of approach. The USNRC guidelines should be subjected to a broad-based, external peer review process including (a) the nuclear industry, (b) other safety-critical industries, and (c) both the commercial and academic software communities.

Recommendation 2. Systems requirements should be written in a language with a precise meaning so that general properties like consistency and completeness, as well as application-specific properties, can be analyzed. Cognizant personnel such as plant engineers, regulators, system architects, and software developers should be able to understand the language.

Recommendation 3. USNRC research in the software quality assurance area should be balanced in emphasis between early phases of the software life cycle and code-level issues. Experience shows the early phases contribute more frequently to the generation of software errors.

Recommendation 4. The USNRC should require a commensurate quality assurance process for ASICs, PLCs, and other similar technologies.

REFERENCES

AECB (Atomic Energy Control Board, Canada). 1996. Draft Regulatory Guide C-138, Software in Protection and Control Systems. Ottawa, Ontario: AECB.

Dijkstra, E.W. 1970. Structured programming. Pp. 84–88 in Software Engineering Techniques, J.N. Buxton and B. Randell (eds.). Brussels: Scientific Affairs Division, NATO.

Fagan, M.E. 1976. Design and code inspections to reduce errors in program development. IBM Systems Journal 15(3):182–211.

Gerhart, S., and L. Yelowitz. 1976. Observations of fallibility in applications of modern programming methodologies. IEEE Transactions on Software Engineering 1(2):195–207.

Goel, A.L., and F.B. Bastani. 1985. Forward: Software reliability. IEEE Transactions on Software Engineering 11(12):1409–1410.

Harel, D., H. Lachover, A. Naamad, A. Pnueli, M. Politi, R. Sherman, A. Shtull-Trauring, and M. Trakhtenbrot. 1990. STATEMATE: A working environment for the development of complex reactive systems. IEEE Transactions on Software Engineering 16(4):403–414.

IEC (International Electrotechnical Commission). 1986. Software for Computers in the Safety Systems of Nuclear Power Stations, IEC 880. Geneva, Switzerland: IEC.

IEEE (Institute of Electrical and Electronics Engineers). 1993. IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2–1993. New York: IEEE.

Joannou, P.K. 1993. Experiences for application of digital systems in nuclear power plants. NUREG/CP-0136. Pp. 61–77 in Proceedings of the Digital Systems Reliability and Nuclear Safety Workshop, U.S. Nuclear Regulatory Commission, September 13–14, 1993, Gaithersburg, Md. Washington, D.C.: US. Government Printing Office.

Lee, E.J. 1994. Computer-Based Digital System Failures. Technical Review Report AEOD/T94-03. Washington, D.C.: USNRC. July.

Leveson, N.G. 1995. Safeware: System Safety and Computers. New York: Addison-Wesley.

Lions, J.L., L. Lubeck, J.-L. Fauquembergue, G. Kahn, W. Kubbat, S. Levedag, L. Mazzini, D. Merle, and C. O'Halloran. 1996. Ariane 5 Flight 501 Failure: Report by the Inquiry Board. Paris: European Space Agency. July 19.

Moore, J.W., and R. Rada. 1996. Organizational badge collecting. Communications of the Association for Computing Machinery 39(8):17–21.

Musa, J.D., A. Iannino, and K. Okumoto. 1987. Software Reliability: Measurement, Prediction, Application. New York: McGraw-Hill Book Company.

Myers, G. 1979. The Art of Software Tests. New York: John Wiley and Sons.

Newberry, S. 1990. SSICB Review of the Load Sequencers in the Enhanced Power System at Turkey Point Plant, Units 3 & 4. Docket Nos. 50-250 and 50-251, November 5, 1990. Washington, D.C.

NRC (National Research Council). 1993. An Assessment of Space Shuttle Software Development Processes. Aeronautics and Space Engineering Board, National Research Council. Washington, D.C.: National Academy Press.

Parnas, D.L. 1985. Software aspect of strategic defense systems. Communications of the Association for Computing Machinery 28(12):1326–1335.

Parnas, D.L., A.J. van Schouwen, and S.P. Kwan. 1990. Evaluation of safety-critical software. Communications of the Association for Computing Machinery 33(6): 636–648.

Paula, H.M. 1993. Failure rates for programmable logic controllers. Reliability Engineering and System Safety 39:325–328.

Paula, H.M., M.W. Roberts, and R.E. Battle. 1993. Operational failure experience of fault-tolerant digital control systems. Reliability Engineering and System Safety 39:273–289.

Porter, A., H.P. Sly, and L.G. Votta. 1996. A review of software inspections. Pp. 40–77 in Software Process, Advances in Computers 42, M.V. Zelkowitz (ed.). San Diego: Academic Press.

Ragheb, H. 1996. Operating and Maintenance Experience with Computer-Based Systems in Nuclear Power Plants. Presentation at International Workshop on Technical Support for Licensing of Computer-Based Systems Important to Safety, Munich, Germany. March.

Rushby, J. 1993. Formal Methods and the Certification of Critical Systems. Menlo Park, Calif.: SRI International. November.

Rushby, J., and F. von Henke. 1991. Formal Verification of the Interactive Convergence Clock Synchronization Algorithm Using EHDM. Technical Report SRI-CSL-89-3R. Menlo Park: SRI International. August.

Rushby, J., and F. von Henke. 1993. Formal verification of algorithms for critical systems. IEEE Transactions on Software Engineering 19(1): 13–23.

USNRC. 1992. Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 138 to Facility Operating License No. DPR-39 and Amendment No. 127 to Facility Operating License No. DPR-48, USNRC, June 1992. Washington, D.C.: USNRC.

5

Common-Mode Software Failure Potential

INTRODUCTION AND BACKGROUND

Safety systems in nuclear power plants must reliably satisfy their functional requirements. To help achieve this goal, safety systems are designed to be single-failure proof, i.e., no single failure is to prevent safety system actuation if needed, nor shall a single failure cause a spurious activation. Various forms of redundancy are commonly used to achieve this design goal, i.e., to achieve the functional goals in the presence of component failures.

There are two approaches to providing redundant components: active redundancy and standby redundancy. In active redundancy, the outputs of multiple identical components or strings of components, operating in parallel, are compared or selected in some way to determine which outputs will actually be used. If the individual components are each highly reliable and fail independently, then a correct output can be assured with high probability.

To avoid the problem of spurious scrams in a nuclear power plant, the active redundancy may involve multiple channels, all carrying the same kind of information and connected so that no protection action will be taken unless a certain number of these channels trip simultaneously. For example, the output from four parallel strings of identical components might be combined using Boolean logic in such a way that the safety systems are activated when two of the four channels exceed the preset threshold level. In this way, a single channel failure cannot prevent or cause safety system activation.

The second type of redundant design uses standby (or backup) redundancy. In this scheme, one or more spares are available to replace failed components. An example of standby redundancy is switching to an alternate or backup power supply when loss of electrical power is detected. Combinations of active and standby redundancy can also be used.

In both active and standby redundancy, components are designed to implement the same function. If the components are identical, this is called component duplication. Component duplication provides protection against independent failures caused by physical degradation (e.g., wearing out) of the components.

The benefits of component duplication can be defeated by common-cause or common-mode failures. Common-cause failures are multiple component failures having the same cause. Common-mode failures denote the failure of multiple components in the same way, such as stuck open or fail as-is. Common-cause and common-mode failures occur when the assumption of independence of the failures of the components is invalid.

Common-cause failures can occur owing to common external or internal influences. External causes may involve operational, environmental, or human factors. The common cause may also be a (dependent) design error internal to the supposedly independent components.

To protect against common design errors, components with a different internal design (but performing the same function) may be used. This approach is called “design diversity” in this report. Multiple versions of software that are written from equivalent requirements specifications are examples of design diversity. That is, the component requirements are the same, but the way the requirement is achieved within the component may be different. Two pieces of software that compute a sine function but use different algorithms to do so are an example of design diversity. As another example, consider two algorithms where the required function is to determine whether two numbers are equal. One algorithm may compute the ratio of the numbers and the other may compare their differences to some number epsilon which has a value close to zero.

A second type of diversity, which is called “functional diversity” in this report, involves components that perform completely different functions at the component level (although the components may be related in that they are used to satisfy higher-level system requirements). The crucial point is that the component requirements are different. An example of functional diversity is the use of high reactor power to flow ratio to cause a reactor trip using control rods, and high coolant temperature to cause a reactor trip using boron concentration. Diversity in this case involves using different principles of operation or physical principles to satisfy the same or different system-level requirements. In the case of software, functional diversity means that the behavioral requirements for the software are different. For example, one program may check to see whether two numbers are equal and another, functionally diverse, program might select the larger of two numbers.

Note that the components must have different functional requirements to count as functionally diverse. Digital components that have the same functional requirements are not functionally diverse and do not make two separate systems diverse. An example of the latter case is the use of a digital component or components to provide the same protection functions where a diverse means to actually shut down the reactor (such as control rods and soluble neutron absorption) is used. The system-level actuation functions may be physically different (dropping the control rods or injecting a soluble neutron absorber), but if the digital components are performing the same protection functions (detection of the conditions to signal the need for a reactor scram), then the digital components do not have functional diversity.

To summarize:

- Redundancy is the use of duplication or diversity to provide alternate means of performing a required function in the event of failure of an individual item (single failure).
- Redundancy may be active (all results, or components, are used) or standby (some results, or components, are not used until failure occurs).
- Duplication is the use of multiple copies of the same component to provide protection against independent failures caused by physical degradation.
- Design diversity is the use of two or more components with a different internal design but performing the same function.
- Functional diversity is the use of two or more components to achieve different functions at the component level, although the functions may be related in terms of higher-level system requirements.
- Design diversity and functional diversity are used to protect against common-cause or common-mode failures.

This chapter is concerned only with digital components. Design diversity, as defined above, is not extensively practiced in nuclear power plants for analog instrumentation and control; identical components and devices are used in redundant channels. This practice results from a conscious decision that design diversity of the nature suggested for software would introduce counter-productive complexity into the hardware environment. Analog systems are believed to fail in more predictable and obvious ways than do the more hidden and insidious failure mechanisms in software. This fact has allowed assessment and protection against common-mode analog failure potential without use of diversity except in a very limited way. It also allows the industry to collect operating experience on failure modes over a large application base.

Digital technology introduces a possibility that common-mode software failure may cause redundant safety systems to fail in such a way that there is a loss of safety function. Arguments for independence in redundant or functionally diverse hardware designs are often based on the failures being related to different physical principles or causes and therefore acceptably independent or on the ability to build in a particular failure mode, e.g., a valve that is designed to fail open. These same arguments and methods do not apply to software. When considering common-mode software failure, the issue is whether assumptions about independence could be compromised when digital components are substituted for analog components.

Although the committee found that some people use the term “common-mode software error” to mean any software error, the term as used here specifically denotes errors that involve dependencies between two or more digital components. When only one of a set of diverse components is digital, i.e., when a digital component is used in conjunction with analog devices or human backups (e.g., when a relay system, a digital device, and a manual actuator are used together to provide design diversity and adequate reliability), there appear to be no additional issues raised over current practice. The committee sees nothing special concerning the common-mode failure problem in this situation that is not covered by current procedures to evaluate the potential for common-mode failure between different types of devices.

Statement of the Issue

Digital technology introduces a possibility that common-mode software failures may cause redundant safety systems to fail in such a way that there is a loss of safety function. Various procedures have been developed and evolved for evaluating common-mode failure potential in analog devices. Do these same procedures apply to computers and software or are different approaches to ensuring reliability needed? What does software diversity mean? Can it be achieved and assessed and, if so, how? Do techniques exist for assessing common-cause failure and common-mode failure when computers are involved? What are the implications of common-mode software failure for the licensing process and the use of component diversity? Are redundancy and diversity the most effective way to achieve reliability for digital systems?

Applicability to Existing and New Plants

The problem of common-mode software failure is important in both retrofits of digital components into existing plants and in new plant design. In older plants where digital components are being substituted for analog ones, assumptions about the independence of components may have been made in the original licensing basis. If these independence assumptions can be invalidated by the introduction of the digital components, then the safety evaluation must be redone using the new assumptions. In new plants, if the use of digital components can invalidate standard assumptions and procedures for achieving and assessing independence and high reliability, then new procedures may be needed.

U.S. NUCLEAR REGULATORY COMMISSION POSITION

The U.S. Nuclear Regulatory Commission (USNRC) staff has developed the following position with respect to diversity, as stated in the draft branch technical position, Digital Instrumentation and Control Systems in Advanced Plants (USNRC, 1992):

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. The staff considers software design errors to be credible common-mode failures that must be specifically included in the evaluation.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented bases [sic] that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. Diverse digital or nondigital systems are considered to be acceptable means. Manual actions from the control room are acceptable if time and information are available to the operators. The amount and types of diversity may vary among designs and will be evaluated individually.
4. A set of displays and controls located in the main control room shall be provided for manual system-level actuation and control of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

The position for existing plants is the same except that item 4 is not required.

Because the regulatory requirement depends on providing a diverse means of carrying out a safety function, the USNRC has also recently issued guidelines to assess whether sufficient diversity exists between digital systems. The guidelines state (USNRC, 1996) that adequate diversity is assumed to exist if:

1. All of the following are different:
   programming language
   hardware
   function
   signal
   design (including design team), or
2. The digital systems provide a different function but are developed using the same programming language and by the same vendor, or
3. The digital systems have a different vendor but perform the same function ("nameplate" diversity), or
4. Case-by-case review is required for other implementations of diversity.

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

The Canadian Atomic Energy Control Board (AECB) has recently also been developing a position on this issue. Their draft regulatory guide C-138, Software in Protection and Control Systems (also discussed in Chapter 4 above), contains the following policy (AECB, 1996):

> To achieve the required levels of safety and reliability, the system may need to be designed to use multiple, diverse components performing the same or similar functions. For example, AECB Regulatory Documents R-8 and R-10 require two independent and diverse protective shutdown systems in Canadian nuclear power reactors. It should be recognized that when multiple components use software to provide similar functionality, there is a danger that design diversity may be compromised. The design should address this danger by enforcing other types of diversity such as functional diversity, independent and diverse sensors, and timing diversity.

Thus, the AECB draft regulatory guide agrees with the USNRC with respect to recognizing the possibility of common-mode software failure and requiring steps to be taken to reduce that possibility. The difference appears to be that the AECB accepts functional diversity as one means of addressing the common-mode software failure issue but does not mandate it. The USNRC accepts digital systems performing the same function but provided by different vendors.

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

Regulatory agencies in fields other than nuclear power do not, in general, have equivalent policies about common-mode software failure because of the different approach to safety assurance in other industries. Thus simple comparisons can be misleading. In general, in other industries, all components are considered potentially safety-critical and no distinction is made between safety and nonsafety systems except with respect to their potential to contribute to hazards identified in a system hazard analysis. Components whose operation or failure could cause hazards (such as control systems) are treated in the same way as those that could mitigate hazards and, in fact, are considered more important because hazard prevention is given a higher priority than hazard mitigation. No assumptions are made or requirements levied to use protection or shutdown systems—the design approach used must be justified for each system according to the hazard analysis and characteristics of the particular system.

The Federal Aviation Administration (FAA) satisfies the need for guidance in satisfying airworthiness requirements for airborne systems by a series of industry-generated and accepted guidelines reflecting best practices: DO-178B, Software Considerations in Airborne Systems and Equipment Certification. These guidelines are in the form of objectives for software life-cycle processes, descriptions of activities and design considerations for achieving these objectives, and descriptions of the evidence that indicate that the objectives have been achieved. The guidelines are applied in a graded manner that depends on the assessed level of criticality of the software component.

Redundancy or diversity in the software is not required by DO-178B. If the licensee wants to take credit for it, that is, reduce the set of normally required activities for their software development process, they must argue the case and get approval from the FAA. Specifically, DO-178B states with respect to using software design diversity (FAA, 1992):

> The degree of dissimilarity and hence the degree of protection is not usually measurable. Probability of loss of system function will increase to the extent that the safety monitoring associated with dissimilar software versions detects actual errors or experiences transients that exceed comparator threshold limits. Multiple software versions are usually used, therefore, as a means of providing additional protection after the software verification process objectives for the software level have been satisfied.

In summary, the FAA position on the use of software diversity is that the degree of dissimilarity and protection provided by design diversity is not usually measurable and therefore is usually counted only as additional protection above a required level of assurance.

The defense and aerospace industry use MIL-STD-882C (DOD, 1993) or variations of it (for example, NASA standards are based on MIL-STD-882C). This standard requires the use of a formal safety program that stresses early hazard identification and elimination or reduction of associated risk to a level acceptable to the managing authority. Rather than specify a particular safety design approach, such as defense-in-depth, or design features, such as redundancy or diversity, MIL-STD-882C requires that contractors establish a system safety program that includes specific tasks (such as hazard tracking, reviews and audits, hazard analyses, and safety verification) and criteria (such as the use of qualitative risk assessment and an order of precedence for resolving hazards). In contrast to the FAA and some nuclear power standards, software components are not graded as to their criticality and then subjected to different software development procedures, but rather the hazards themselves are assessed and either eliminated or controlled. Earlier versions of this defense standard included tasks that were specific to software, but the latest version (MIL-STD-882C) has integrated the software tasks with the nonsoftware tasks and does not distinguish them.

The U.S. Office of Device Evaluation of the Center for Devices and Radiological Health of the U.S. Food and Drug Administration has issued Reviewer Guidance for Computer Controlled Medical Devices Undergoing 510(k) Review (FDA, 1991). This guidance applies to the software aspects of premarket notification (510(k)) submissions for medical devices. It provides (1) an overview of the kind of information about software that FDA reviewers may expect in company submissions and (2) specification of the approach that FDA reviewers should take in reviewing computer-controlled devices, such as some key questions that will be asked during the review.

The FDA guidance does not dictate any particular approach to safety, as does the USNRC, or specific software development or quality assurance procedures, as does the FAA. Instead, it focuses attention on the software development process to assure that potential hazardous failures have been addressed, effective performance has been defined, and means of verifying both safe and effective performance have been planned, carried out, and properly reviewed. The FDA believes that in addition to testing, device manufacturers should conduct appropriate analyses and reviews in order to avoid errors that may affect operational safety.

The depth of review is dictated by both the risk to the patient of using (and not using) the device and the role that software plays in the functioning of the device. The three levels of concern are (FDA, 1991):

> MAJOR: The level of concern is major if operation of the device or software function directly affects the patient so that failures or latent design flaws could result in death or serious injury to the patient, or if it indirectly affects the patient (e.g., through the action of a care provider) such that incorrect or delayed information could result in death or serious injury of the patient.
>
> MODERATE: The level of concern is moderate if the operation of the device or software function directly affects the patient so that failures or latent design flaws could result in minor to moderate injury to the patient, or if it indirectly affects the patient (e.g., though the action of a care provider) where incorrect or delayed information could result in injury of the patient.
>
> MINOR: The level of concern is minor if failures or latent design flaws would not be expected to result in death or injury to the patient. This level is assigned to a software component that the manufacturer can show to be totally independent of other software or hardware that may be involved in a potential hazard and would not directly or indirectly lead to a failure of the device that could cause a hazardous condition to occur.

The FDA does not specify particular software assurance or development procedures. Instead, the FDA specifies what information should be included in the review documents and what types of questions will be asked during the review for each level of concern. The submission must include a hazard analysis that identifies the potential hazards associated with the device, the method of control (hardware or software), the safeguards incorporated, and the identified level of concern. Because there is no specification of how safety should be achieved, there is no guidance provided on redundancy or diversity.

U.S. NUCLEAR REGULATORY COMMISSION RESEARCH ACTIVITIES

The Office of Nuclear Regulatory Research of the USNRC indicated that they currently fund only one research project on common-mode failure potential. This research project is developing a software tool called Unravel for program slicing.

Program slicing is a technique that was developed to assist with software debugging. Basically, program slicing extracts the statements that might affect the value of a specified variable before execution reaches a particular statement in the program. Thus, if one is trying to fix an error in statement N, it is helpful to know what other statements in the software can affect the values of the variables in that statement.

To perform the slicing, the program is first represented as a flow graph annotated with the variables referenced and defined at each node (roughly, a node is a programming language statement). Unravel works only on programs written in the (ANSI [American National Standards Institute]) C programming language, without any extensions to the language. Some features of C cannot be handled, including calls to the C standard library.

The USNRC argument for the usefulness of this tool is that it can assist auditors in evaluating functional diversity in safety-critical software and in conducting a thread audit. The committee has not previously seen any argument that the technique could be used for evaluating diversity and are skeptical about this (see the evaluation later in this chapter).

ANALYSIS

When multiple digital components are used to provide diversity, the potential for common-mode software failure exists, requiring consideration of two relevant issues: (1) whether failure independence can be assumed or under what conditions it can be assumed (Issue 1); and (2) whether failure independence can be verified, that is, whether there are any ways to determine that the digital components are adequately independent or diverse in their failure behavior (Issue 2). Both issues are examined in turn, considering both digital hardware and software.

Issue 1

Is the failure independence assumption justified for independently produced digital components? For the purposes of discussing this question, design diversity is separated from functional diversity. Also, operating systems are grouped with hardware unless the operating system functions have been specially written for a particular application or digital device. In the latter case, operating systems are considered as application software.

Design Diversity

Case 1: Digital Hardware and Operating Systems. For hardware, the prevalence of a very few processors and real-time operating systems invalidates the use of simple “name-plate” diversity assumptions. Many computers with different manufacturers in fact have identical internal components or use the same operating system.

Although the committee knows of no data to support generally rejecting the assumption of independence between failures of diverse digital hardware devices, there are three concerns in assuming independent failures between digital hardware components providing the same function but produced by different manufacturers. The first is that many of the well-publicized errors found in processors have involved similar functions, for example, floating point operations. The second is the increasing complexity of chip designs, which has led to a lowered ability to adequately test the designs before using them. Testing and verification techniques originally developed for software are now being adapted for use in digital hardware because the complexity of these hardware designs is approaching that of software, thus defying exhaustive testing. A third consideration is the use of common design environments, libraries, and fabrication facilities.

Therefore, the question of whether hardware design errors can be assumed to be independent is beginning to have a close relationship to the same question with respect to software. Currently, however, when the design is different there exists no evidence to invalidate the assumption that failures of digital hardware components due to design errors will be independent.

Similarly, assuming intended differences in design, there also is little current evidence to invalidate an assumption of independence of failure between different real-time operating systems. Note, however, that this assumption applies only to operating systems developed by different companies. Different versions of an operating system by one vendor often include the reuse of much of the same code. In addition, evidence does exist of similar failure modes and errors being found in UNIX operating systems built by different vendors (Miller et al., 1990).

However, the above restrictions may be relaxed if analysis has shown that there is functional diversity. This would allow a single company to design functionally diverse operating systems. Similarly, functional diversity needs to be assured when using different companies for operating systems and hardware. Licensing agreements between companies can destroy assumptions of functional diversity based on different vendors.

However, even operating systems and library functions produced by different companies can have common-mode software errors. For example, in 1990, a mathematician reported on a computer bulletin board that he had found a serious bug in MACSYMA, a widely used program that computes mathematical functions (Sci.math, 1990). This program incorrectly computes the integral from 0 to 1 of the square root of (x + 1/x – 2) to be –(4/3) instead of the correct value of 4/3. Other readers of the bulletin board became curious and tried the same problem on other math packages. The result was that four packages (MACSYMA, Maple, Mathematica, and Reduce) got the same wrong answer while only one (Derive) got the correct answer. These mathematical packages were all developed separately in different programming languages, and even in different countries, and had been widely used for many years and yet contained the same error.

Case 2: Application Software. The effectiveness of design diversity in increasing software reliability rests on the assumption of statistical independence of failures in separately developed software versions (including both application software and specially constructed operating system functions), such as separately developed digital protection systems. This assumption is important in evaluating whether software design diversity satisfies the USNRC requirements for diversity and independent failures.

Several scientific studies have experimentally evaluated the hypothesis that software separately developed to satisfy the same functional requirements will fail in a statistically independent manner (Brilliant et al., 1990; Eckhardt et al., 1991; Knight and Leveson, 1986; Scott et al., 1987). All these studies have rejected the hypothesis with a high confidence level, i.e., concluded that the number of correlated (common-mode) failures that actually occurred for the programs in the various experiments could not have resulted by chance. The implication is that although design diversity might be able to increase reliability, increased reliability cannot be assumed.

In two of the experiments, the programming errors causing correlated (common) failures were examined to better understand the nature of faults that lead to coincident failures and to determine methods of development for multiple software versions that would help avoid such faults. The first experiment (Knight and Leveson, 1986) found that, as anticipated, in some cases the programmers made equivalent logical errors. More surprising, there were cases in which apparently different logical errors yielded correlated failures in completely different algorithms or in different parts of similar algorithms. For example, in order to satisfy the requirements, the programs needed to compute the size of an angle given three points. Most of the programs worked correctly for the normal case. However, eight of the 27 programmers had difficulty in handling the case where three points were collinear, even though the algorithms used and the actual errors made were quite different. Five of the eight mishandled or failed to consider one or both of the possible subcases (i.e., angle equal to zero degrees and angle equal to 180 degrees). One handled all the cases, but used an algorithm that was inaccurate over certain parts of the input space. Another had machine round-off problems. The final programmer had an apparent typo in an array subscript that, seemingly by chance, resulted in an error only when the points were collinear. Knight and Leveson concluded that there are some input cases (i.e., parts of the problem space) that are more difficult to handle than others and are therefore likely to lead to errors, even though the algorithms used and the actual errors made may be very different. The second experiment (Scott et al., 1987) examined the errors made in the programs in their experiment and also concluded that dependence was related to a "difficulty factor": If one program gave a wrong answer for a particular input, then it was likely that other programs would also produce an incorrect answer, even though the errors made were different and the programs used different algorithms.

In another experiment, Brunelle and Eckhardt (1985) took a portion of an operating system (SIFT) and ran it in a three-way voting scheme with two other operating systems written for the same computer. The results showed that although no errors were found in the original version, there were instances where the two new versions outvoted the correct original version to produce a wrong answer.

Following these experiments, Eckhardt and Lee (1985) produced a mathematical model that explains the results. Their model also shows that even small probabilities of correlated failures, i.e., deviation from statistically independent failures, cause a substantial reduction in potential reliability improvement when using diverse software components.

In summary, the experiments conducted on this issue indicate that statistically correlated failures result from the nature of the application, from similarities in the difficulties experienced by individual programmers, and from special cases in the input space. The correlations seem to be related to the fact that the programmers are all working on the same problem and that humans do not make mistakes in a random fashion.

There is no reason to expect that the use of different development tools or methods, or any other simple technique, will reduce significantly the incidence of errors giving rise to correlated failures in multiple-version software components. All evidence points to the fact that independently developed software that uses different programmers, programming languages, and algorithms but computes the same function (satisfies the same functional requirements) cannot be assumed to fail in an independent fashion. Thus the USNRC position that allows "nameplate" diversity or design diversity to be used to assure independence is not supported by the extensive scientific evidence that is available. Other regulatory agencies, such as the FAA and the AECB, do not accept design diversity as evidence of failure independence.

Functional Diversity

In contrast with design diversity, no assumptions about the independence of the code are made when using functional diversity, only about whether the functional requirements are independent and different. The problem here really reduces to the same problem that is found with functionally diverse analog components, and no new procedures are necessary except to determine whether any new failure modes have been introduced that might violate the system-level independence assumptions. Thus, the current USNRC position on functional diversity is consistent with the scientific evidence.

Issue 2

Can the independence of multiple versions of software be evaluated? That is, if the assumption of statistical independence cannot simply be assumed in independently developed software, can software diversity be evaluated or assessed in some way?

Procedures have been developed for evaluating the potential for common-mode failure of analog hardware components. In addition, the number of states and the continuity of behavior over the total state space for analog components allows either exhaustive testing or much more confidence in the testing. In contrast, only a small fraction of the state space for digital systems can usually be tested and the lack of continuity in behavior does not allow any assumptions about the behavior of the software for any inputs or input sequences not specifically tested.

Verifying diversity between two algorithms is impossible in general. Equivalence between two algorithms (and thus also lack of equivalence) has been proven to be mathematically undecidable. But even if diversity cannot be assessed formally, perhaps it can be evaluated informally. The problem reduces to determining what is meant by design diversity between two computer programs. Syntactic diversity (differences in the syntax or lexical structure of the programs) is not the relevant issue: Two programs can be syntactically different (look very different) and yet compute identical mathematical functions.

Even if one *could* verify diversity between two algorithms, that would not be adequate, because different algorithms may compute the same functions and therefore behave identically. Basically, what is sought is two programs that compute the same function except where they are incorrect (i.e., where they differ from the requirements). Evaluating for independence of failure behavior would require proving that the two programs were different only in their failure behavior (or that they were not identical in their total function computed). To accomplish this would require the same logical power as that required to identify design errors (at which point they would just be removed). Thus, if it were possible to verify effective design diversity, diversity would not be needed. In summary, there is no way to verify or evaluate the diversity of two software versions or to determine whether they will fail independently.

As discussed earlier, the USNRC currently is funding a research project at the National Institute of Standards and Technology to build a tool called Unravel for program slicing. A stated goal for this tool is to assist USNRC auditors in evaluating functional diversity in nuclear power plant safety system software. The developers of the tool say that it can be used to "identify code that is executed in more than one computation and [that] thus could lead to a malfunction of more than one logical software component."

In general, evaluating functional diversity is not possible by simply identifying the code related to a particular computation, as done by program slicing. The probability that separately developed programs will contain the same code is extremely small. If there is any attempt to make the software diverse, then the programs will almost certainly use different variables, data structures, and algorithms. In addition, the experiments described above found that programs failed in a statistically dependent manner even when they used completely different algorithms and had unrelated programming errors. The only relationship needed between software errors to cause statistically dependent failures is that the errors occur on the execution paths for each program that will be followed by the same input data. The errors can appear anywhere on those paths, and the computations and errors on the paths may be different.

The second proposed use of program slicing is for thread audits. However, a technique like program slicing that works backward from a particular statement to find any statements that might affect it seems to have much less relevance for thread audits than a tool that will identify paths through the code starting from particular inputs. Other techniques, such as symbolic execution, are more precise (provide more information to the analyst) and are probably less costly. Slicing can work backward from an output to identify statements affecting the output and thus all paths to that output, but cannot distinguish feasible from infeasible paths and identifies all such paths, not just those related to a particular input. The analyst must then by hand determine which paths relate to the thread being investigated and determine whether the path is feasible (a difficult task). Symbolic execution, on the other hand, can start from specific inputs and identify feasible paths through the code, evaluating the particular predicates that must be true for the path to be taken. Another potentially useful technique related somewhat to symbolic evaluation, called Software Deviation Analysis (Reese, 1996), also does a forward analysis from inputs to determine the effect on outputs, but starts with likely or possible deviations in the inputs from their expected values and determines whether hazardous outputs can be generated.

Alternatives to Diversity for Software

In addition to the two main diversity issues discussed above (Issue 1 and Issue 2), one final question is whether redundancy and diversity are the most effective way to increase reliability for digital systems or whether there are more effective alternatives. Potential alternatives include mathematical verification techniques, self-checking software, and safety analysis and design techniques.

While mathematical verification of software is potentially effective in finding programming errors, these techniques are difficult to use and have only been applied to very small programs by mathematically sophisticated users. The difficulty of writing the required formal specifications and doing the proofs has not been shown to be less error prone in practice than using less formal techniques. In fact, little or no comparative evaluation with the alternatives has been done. Despite these caveats, the committee notes that mathematical verification has been used by Ontario Hydro on their Darlington and Pickering plant protection system software. The committee understands that the Canadian experience shows that mathematical verification costs can be very high but is far more cost effective if it is built into the development process from the beginning rather than being imposed at the end.

Digital systems have the capability to provide self-checking to detect digital hardware failures and some software errors during execution. This has proven effective for random hardware failures but not for software design errors. Built-in tests for some programming errors, such as attempting to divide by zero, are easily implemented and effective. However, checking for more subtle errors is more difficult and may, in itself, add so much complexity that it leads to errors. For example, a licensee event report about a problem at the Turkey Point plant in Florida in 1994 described a software error that could result in a real emergency signal being ignored if it is received 15 seconds or more after the start of particular test scenarios (see discussion in Chapter 4). An experiment by Leveson et al. (1990) in writing self-checks for software found that very few of the known errors in the code were found by the self-checks. Even more discouraging, the self-checks themselves introduced more errors than they found.

Safety analysis and design techniques (see Leveson, 1995) extend standard system safety techniques to software. Software-related hazards are identified and then eliminated or controlled. In this approach, not all potential errors are targeted but simply those that could lead to hazards or accidents. As such, this approach is potentially less costly than a full formal verification. A type of safety verification procedure (called software fault tree analysis) was used (in addition to formal verification) during the licensing of the Darlington shutdown system (Bowman et al., 1991). The information provided during the analysis was used to change the code to be more fault-tolerant and to design 40 self-checks that were added to the software.

Although many in the software engineering community believe that there are more cost-effective techniques (including both those described here and others) for achieving high software reliability than redundancy and diversity, there is no agreement among them about what these alternatives are.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. The USNRC position of assuming that common-mode software failure could occur is credible, conforms to engineering practice, and should be retained.

Conclusion 2. The USNRC position with respect to diversity, as stated in the draft branch technical position, Digital Instrumentation and Control Systems in Advanced Plants, and its counterpart for existing plants, is appropriate.

Conclusion 3. The USNRC guidelines on assessing whether adequate diversity exists need to be reconsidered. With regard to these guidelines: (a) The committee agrees that providing digital systems (components) that perform different functions is a potentially effective means of achieving diversity. Analysis of software functional diversity showing that independence is maintained at the system level and no new failure modes have been introduced by the use of digital technology is no different from that for upgrades or designs that include analog instrumentation. (b) The committee considers that the use of different hardware or real-time operating systems is potentially effective in achieving diversity provided functional diversity has been demonstrated. With regard to real-time operating systems, this applies only to operating systems developed by different companies or shown to be functionally diverse. (c) The committee does not agree that use of different programming languages, different design approaches meeting the same functional requirements, different design teams, or different vendors' equipment used to perform the same function is likely to be effective in achieving diversity. That is, none of these methods is a proof of independence of failures. Conversely, neither is the presence of these proof of dependence of failures.

Conclusion 4. There appears to be no generally applicable, effective way to evaluate diversity between two pieces of software performing the same function. Superficial or surface (syntactic) differences do not imply failure independence, nor does the use of different algorithms to achieve the same functions. Therefore, funding research to try to evaluate design diversity does not appear to be a reasonable use of USNRC research funds.

Conclusion 5. Although many in the software community believe that there are more cost-effective techniques for achieving high software reliability than redundancy and diversity, there is no agreement as to what these alternatives may be. The most promising of these appear to be the extension of standard safety analysis and design techniques to software and the use of formal (mathematical) analysis. (See Recommendation 3 in Chapter 4.)

Conclusion 6. The use of self-checking to detect hardware failures and some simple software errors is effective and should be incorporated. However, care must be taken to assure that the self-checking features themselves do not introduce errors.

Recommendations

Recommendation 1. The USNRC should retain its position of assuming that common-mode software failure is credible.

Recommendation 2. The USNRC should maintain its basic position regarding the need for diversity in digital instrumentation and control (I&C) systems as stated in the draft branch technical position, Digital Instrumentation and Control Systems in Advanced Plants, and its counterpart for existing plants.

Recommendation 3. The USNRC should revisit its guidelines on assessing whether adequate diversity exists. The USNRC should not place reliance on different programming languages, different design approaches meeting the same functional requirements, different design teams, or using different vendors' equipment ("nameplate" diversity). Rather, the USNRC should emphasize potentially more robust techniques such as the use of functional diversity, different hardware, and different real-time operating systems.

Recommendation 4. The USNRC should reconsider the use of research funding to try to establish diversity between two pieces of software performing the same function. This does not appear to be possible. Specifically, it appears the USNRC funding of the Unravel tool is based on the use of this tool for this purpose and, as such, is unlikely to be useful.

REFERENCES

AECB (Atomic Energy Control Board, Canada). 1996. Draft Regulatory Guide C-138, Software in Protection and Control Systems. Ottawa, Ontario: AECB.

Bowman, W.C., G.H. Archinoff, V.M. Raina, D.R. Tremaine, and N.G Leveson. 1991. An Application of Fault Tree Analysis to Safety-Critical Software at Ontario Hydro. Presentation at Conference on Probabilistic Safety Assessment and Management (PSAM), Beverly Hills, Calif., April.

Brilliant, S., J.C. Knight, and N.G. Leveson. 1990. Analysis of faults in an N-version software experiment. IEEE Transactions on Software Engineering 16(2):238–247.

Brunelle, J.D., and D.E. Eckhardt. 1985. Fault-Tolerant Software: Experiment with the SIFT Operating System. Presentation at AIAA Computers in Aerospace Conference, Dallas, October.

Eckhardt, D.E., and L. Lee. 1985. A theoretical basis for the analysis of multiversion software subject to coincident errors. IEEE Transactions on Software Engineering 11(12):1511–1517.

Eckhardt, D.E., A.K. Caglayan, P. Lorczak, J.C. Knight, D.F. McAllister, M. Vouk, L. Lee, and J.P. Kelly. 1991. Robustness of software redundancy as a strategy for improving reliability. IEEE Transactions on Software Engineering 17(7):692–702.

DOD (U.S. Department of Defense). 1993. Military Standard 882C, System Safety Program Requirements. Washington, D.C.: U.S. Department of Defense.

FAA (Federal Aviation Administration). 1992. DO-178B, Software Considerations in Airborne Systems and Equipment Certification. Washington, D.C.: FAA.

FDA (Food and Drug Administration). 1991. Reviewer Guidance for Computer Controlled Medical Devices Undergoing 510(k) Review. Washington, D.C.: FDA.

Knight, J.C., and N.G. Leveson. 1986. An experimental evaluation of the assumption of independence in multi-version programming. IEEE Transactions on Software Engineering 12(1):96–109.

Leveson, N.G. 1995. Safeware: System Safety and Computers. New York: Addison-Wesley.

Leveson, N.G, S.S. Cha, J.C. Knight, and T.J. Shimeall. 1990. The use of self checks and voting in software error detection: An empirical study. IEEE Transactions on Software Engineering 16(4):432–443.

Miller, B.P., L. Fredrikson, and B. So. 1990. An empirical study of the reliability of UNIX utilities. Communications of the Association for Computing Machinery 33(12):32–44.

Reese, J.D. 1996. Software Deviation Analysis. Ph.D. dissertation, University of California, Irvine. January.

Sci.math. 1990. Various authors posting to this Usenet newsgroup, Feb. 3–8.

Scott, R.K., J.W. Gault, and D.F. McAllister. 1987. Fault tolerant reliability modeling. IEEE Transactions on Software Engineering 13(5):582–592.

USNRC (U.S. Nuclear Regulatory Commission). 1992. Draft Branch Technical Position on Digital Instrumentation and Control Systems in Advanced Plants. Washington, D.C.: USNRC.

USNRC. 1996. Draft Branch Technical Position on Defense-in-Depth and Diversity. Washington, D.C.: USNRC. (Also USNRC staff presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., October 1995.)

6

Safety and Reliability Assessment Methods

INTRODUCTION

Appropriate methods for assessing (as distinct from achieving or assuring) safety and reliability are the key to establishing the acceptability of digital instrumentation and control (I&C) systems in nuclear plants. Methods must be available to support estimates of reliability, assessments of safety margins, comparisons of performance with regulatory criteria such as quantitative safety goals, and overall assessments of safety in which trade-offs are made on the basis of the relative importance of disparate effects such as improved self-checking acquired at the cost of increased complexity. These methods must be sufficiently robust, justified, and understandable to be useful in assuring the public that using digital I&C technology in fact enhances public safety.

Statement of the Issue

Effective, efficient methods are needed to assess the safety and reliability of digital I&C systems in nuclear power plants. These methods are needed to help avoid potentially unsafe or unreliable applications and aid in identifying and accepting safety-enhancing and reliability-enhancing applications. What methods should be used for making these safety and reliability assessments of digital I&C systems?

Discussion

In nuclear power plants, reliability and safety are assessed using an interactive combination of deterministic and probabilistic techniques. The issues that the committee considered were the extent to which these assessment methods are applicable to digital I&C systems and the appropriate use of these methods.

Deterministic Techniques

Design basis accident analysis is a deterministic assessment of the response of the plant to a prescribed set of accident scenarios. This specific analysis constitutes a major section of the nuclear plant safety analysis report that is submitted to and reviewed by the U.S. Nuclear Regulatory Commission (USNRC) in the licensing process. In a design basis accident analysis an agreed-upon set of transient events are imposed on analytical simulations of the plant. Then, assuming defined failures, the plant systems must be shown to be effective in keeping the plant within a set of defined acceptance criteria. Consider, for example, the analysis of the thermal response of the reactor following a postulated pipe rupture. In this case, the deterministic safety analysis considers:

- the size of the rupture (the cross-sectional area of the pipe)
- the geometry of the systems and components affected, such as volumes and elevations of pipes and vessels
- the initial conditions (conditions at the time of the rupture), such as initial power, pressures, and temperatures
- the response logic of the active and passive safety systems, such as the sensing of the event by the instrumentation systems, the subsequent actuation of valves that isolate the fault, and the subsequent opening of backup feedwater system valves

All these considerations are used as parameters or forcing functions in the equations that model the physical behavior of the affected systems (mainly nuclear, thermal, mass, and momentum conservation equations) to calculate the response of the system. Of particular importance is the calculation of the resultant pressures and temperatures in the cooling systems and in the core to assess the integrity of the fuel and the multiple physical barriers that contain radionuclides.

Probabilistic Techniques

Probabilistic risk assessment (PRA) (or probabilistic safety assessment [PSA]) techniques are used to assess the relative effects of contributing events on system-level safety or reliability. Probabilistic methods provide a unifying means of assessing physical faults, recovery processes, contributing effects, human actions, and other events that have a high degree of uncertainty. These analyses are typically performed using fault tree analysis; but other methods, such as event trees, reliability block diagrams, and Markov methods, are also appropriate. In PRA, the probability of occurrence of various end events, both acceptable and unacceptable, is calculated from the probabilities of occurrence of basic events (usually failure events). For example, the USNRC has established a quantitative safety goal that the probability of a core damage event shall not exceed 10^{-5} per reactor year. The results of a particular PRA, of course, have wide bands of uncertainty; but on a relative basis they allow searching out the most important failure modes ("weak points") and allow the designer to balance the design appropriately between mitigation and prevention and to avoid unhealthy dependence on single systems or components.

The development of a fault tree model serves several important purposes. First, it provides a logical framework for analyzing the failure behavior of a system and for precisely documenting which failure scenarios have been considered and which have not. Second, the fault tree model has a well-defined Boolean algebraic and probabilistic basis that relates probability calculations to Boolean logic functions. That is, a fault tree model not only shows how events can combine to cause the end (or top) event, but at the same time defines how the probability of the end event is calculated as a function of the probabilities of the basic events. Thus the fault tree model can evolve as the system evolves and can at any time evaluate the effect of proposed changes on the reliability and safety of the nuclear power plant. In this manner the fault tree analysis can be used to support engineering tasks such as illuminating the design "weak points," facilitating trade-off analyses, or assessing relative risks.

As mentioned above, the probabilistic analysis of reliability and safety is dependent upon an assignment of a probability of occurrence for each basic event in the fault tree. In addition to addressing the probability of an event, however, probability analysis may also address probabilities of variability and uncertainty. For example, an estimation may be made of the probability that a component will fail (probability of an event). But this failure probability may vary as a result of statistical variation in external conditions, such as temperature, or statistical characteristics of the source of the component. A second probability concept describes this variation as a probability distribution around a "point estimate" for the failure probability. Furthermore, the failure probability may not be known with perfect confidence. A third probability concept uses a distribution to express the degree of uncertainty associated with the point estimate reflecting the differences and uncertainties among experts solicited for judgments on probabilities (see below). Thus current risk assessment practice distinguishes between probabilities of events, variability, and uncertainty (NRC, 1994).

An uncertainty analysis using the fault tree model reflects the degree to which the output value is affected by the uncertainty in an input. This analysis helps the designer determine the extent to which an unknown input can affect the reliability or safety of the system and thus the extent to which the system must be able to withstand such uncertainty (Modarres, 1993).

But the fundamental concept in probabilistic analysis remains the concept of the probability of an event. There are several interpretations of the probability associated with an event (Cooke, 1991; Cox, 1946; McCormick, 1981; Modarres, 1993). The classic notion of the probability of an event is the ratio of the size of the subspace of sample points that include the event to the size of the sample space. A frequency interpretation of the probability of an event is the one most commonly understood; it defines the probability of an event as the limit of the ratio of the number of such events observed to the number of trials as the number of trials becomes large. Many events considered in a probabilistic safety assessment in the nuclear field are, however, classifiable as rare events, which complicates the estimation of occurrence probabilities for the basic events. If failure probabilities are to be estimated from life testing or field experience, many samples must be studied over long periods of time in order to gain any statistical significance in the data (Leemis, 1995). Several databases and handbooks exist to help with the estimation of failure probabilities for basic events (Bellcore, 1992; DOD, 1991; Gertman and Blackman, 1994; RAC, 1995). Within the nuclear engineering community, failure data for nuclear-specific systems and components are available from several sources, including summaries of licensee event reports (USNRC, 1980, 1982a, 1982b) and other handbooks (IEEE, 1983; USNRC, 1975). The existence and use of such handbooks helps address the problems associated with obtaining failure data for many of the basic events.

But for some basic events, where there are few or no applicable data on frequencies, subjective interpretations of probability may be used and may, in fact, be all that is available. Subjective probabilities may be sought in formal and informal processes in which groups of experts weigh available evidence and make judgments. This approach to probability is not of course based on relative frequencies and does not require samples or trials except as they may be available to inform subjective engineering judgment. Rather, subjective interpretations are commonly described as measures of the degree of belief that an event will occur. For example, Apostolakis (1990) states that "probability is a measure of belief." He continues: "The primitive notion is that of 'more likely': that is, we can intuitively say that event A is more likely than event B. Probability is simply a numerical expression for this likelihood." However, as more information becomes available, the subjective distribution (see discussion of uncertainty analysis above) can be adjusted to reflect the current state of knowledge.

There is extensive experience in nuclear risk studies and elsewhere with such elicitation of expert judgments on probabilities. Bayesian analysis (Leemis, 1995) tells how past observations (i.e., frequency data) influence the subjective judgment. Certain characteristic biases, such as tendencies toward overconfidence, are known to occur (Cooke, 1991). Notwithstanding its limitations, the subjective interpretation of probability is the usual basis for the analysis of rarely occurring events and forms the basis of many risk evaluations (McCormick, 1981). As such, it is important to the committee's consideration of the applicability of probabilistic analysis to digital systems.

Hazard analysis (i.e., experts thinking about what might go wrong) has been validated as effective for at least 50 years. Random testing has been suggested as an alternate approach. However, truly random testing is not particularly good for finding hazards as it is more of a "needle-in-a-haystack" approach. Tests might also be randomly generated from an abstract description of a rare-event scenario. However, significant expertise is needed to formulate such a description.

Applicability to Digital Systems

Deterministic analysis techniques for digital systems are a generalization of the design basis accident methodology used in the nuclear industry and include such techniques as hazard analysis and formal methods (Leveson, 1995; Rushby, 1995). The use of deterministic analysis techniques for the analysis of digital systems is not controversial, as long as they are applied with care to consider the failure modes attributable to digital systems. More controversial is the applicability of probabilistic models to digital systems. The committee spent much of its effort on this issue in assessing the applicability of probabilistic analysis methods to digital systems.

Although well-accepted techniques exist for the analysis of physical faults, probabilistic analysis of design faults in critical systems is more problematic. Because software faults are by definition design faults, the discussion will focus on probabilistic techniques for assessing software. It should be noted that much of the discussion is applicable to similar systems that may be implemented in hardware, using programmable devices or application-specific integrated circuits.

There is controversy within the software engineering community as to whether software fails, whether it fails randomly, and whether the notion of a software failure rate exists. Some would assert that software does not "fail" because it does not physically change when an incorrect result is produced. Others assert that software either works or does not work, and thus its reliability is either zero or one (see, e.g., Singpurwalla, 1995, and the published discussion accompanying that reference).

Some who accept the notion of software failure disagree as to whether software failure can be modeled probabilistically. Some argue that software is deterministic, in that given a particular set of inputs and internal state, the behavior of the software is fixed. The most common justification for the apparent random nature of software failures is the randomness or uncertainty of the input sequences (Eckhardt and Lee, 1985; Laprie, 1984; Littlewood and Miller, 1989). For example, Finelli (1991) identifies "error crystals" (regions of the input space that cause a program to produce errors); a software failure occurs when the input trajectory enters an error crystal. Recent experimental work (Goel, 1996) seems to suggest that the reliability of some software can be modeled stochastically as a function of the workload.

For non-safety-critical software systems, statistical analysis techniques are being used in the software reliability engineering process (Lyu, 1996). For example, the statistical analysis of the results (i.e., detected failures) of a good set of tests can, based on the operational profile, help managers answer questions such as "When can I release this version?" or "When can I consider this phase of testing complete?" The basic premise is that a set of random tests of a large software system provides data as to the probability of failure for a particular version of software.

Many of the methods developed for software reliability engineering of large-scale commercial systems are not directly applicable to embedded systems for critical applications. One problem with the software reliability engineering approaches is that a very large number of test cases must be considered to statistically validate a low probability of failure (Butler and Finelli, 1993).

For very reliable software, the software would be expected to pass every test, making statistical analysis even more difficult. If software for a safety-critical application were to fail a test, the software would be changed in such as way as to correct the error and the testing would be restarted. Thus, a point would be reached when the software would have passed a very large number of tests. Miller et al. (1992) describe several methods for estimating a probability of failure for software that, in its current version, has not failed during random testing. Bertolino and Strigini (1996) propose a method for estimating both the probability of failure and the probability of program correctness from a series of failure-free test executions. Parnas et al. (1990) describe a methodology for determining how many tests should be passed in order to achieve a certain level of confidence that the failure probability is below a specified upper bound. A similar approach is described in NUREG/CR-6113 (USNRC, 1993a). In this case, the operating range of a safety system is considered to be the transition region between safe and unsafe operation. Thus it is recommended that random tests be selected in this transition region, and a mathematical formula is given for determining the number of test cases needed for statistical confidence that the failure probability is below a given upper bound.

The validity of these methods is dependent on the quality of the test cases chosen. The test cases should be representative of the inputs encountered in practice and should certainly include all boundary conditions and known potentially hazardous cases. Random testing should, however, be only a part of a complete program for safety assessment and quality assurance, a program that includes formal methods (Rushby, 1995) or other analysis techniques throughout the development and assurance process. Testing and formal methods, besides being complementary, can be mutually supportive as well. Analysis can help determine potentially hazardous conditions that should be tested, and testing can help validate critical assumptions made in the analysis (Walter, 1990).

Some failure data from operational systems in the nuclear and other industries are available (Paula, 1993). Failure rates for microprocessor-based programmable logic controllers used in emergency shutdown systems are reported by Mitchell and Williams (1993). Fault-tolerant digital control systems failures are analyzed by Paula et al. (1993), who also present a quantitative fault tree analysis that helped a group of owners decide whether to replace existing analog control systems with fault-tolerant digital control systems. In 90 system years of operation, 279 single-channel failures and 55 multiple-channel failures were reported. Of the 55 multiple-channel failures, nine were attributed to software deficiencies. The fault tree analysis included such failure modes as inadvertent operator actions, software failures, physical damage from external events, lack of coverage, and hardware component and communication failures.

CURRENT U.S. NUCLEAR REGULATORY COMMISSION REGULATORY POSITION AND PLANS

The criteria under which a utility can make plant changes without prior USNRC approval are established in 10 CFR 50.59. One of the specified criteria for determining whether a change requires approval (i.e., involves an unreviewed safety question) is whether the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased.

The USNRC is increasingly incorporating probabilistic risk assessment into all of its rulemaking activities as it develops a risk-informed, performance-based stance (Newman, 1995). The current USNRC regulatory position on the probabilistic analysis of digital systems, however, is not clearly established or well documented. In an October 1995 presentation to the committee, USNRC staff described their position as follows (USNRC, 1995a): "It is the responsibility of the licensees to ensure appropriate reliability and safety of the digital I&C system. The design life-cycle activities permit both qualitative and quantitative methodologies for assessing reliability and are sufficiently adaptable to consider the evolving aspect of digital technology." However, although qualitative software assurance techniques are presented in several NUREG publications prepared by the Lawrence Livermore National Laboratory (USNRC, 1993b, 1995b), these contain no discussion of probabilistic analysis. In fact, in the October 1995 presentation, the USNRC staff also stated that "quantitative reliability assessment methods for digital systems are not believed to be sufficiently developed to be acceptable as standard practice" (USNRC, 1995a). In further discussions with the committee in April 1996, in addressing the evaluation of relative frequencies of occurrence for use in 10 CFR 50.59 determinations, the USNRC staff indicated they did not consider current evaluation methods to be sufficiently accurate to be meaningful (USNRC, 1996b).

DEVELOPMENTS IN THE U.S. NUCLEAR INDUSTRY

In the U.S. nuclear industry, the use of probabilistic analysis for digital systems (particularly software) is mixed. The analysis of a fault-tolerant digital control system by Paula et al. (1993) used a fault tree and included software failures; however, this approach is not common. A discussion of key assumptions and guidelines for PRA from the Electric Power Research Institute's Utility Requirements Document (EPRI, 1992) shows no mention of software or of failure modes peculiar to digital systems. When several industry representatives were asked by the committee about the use of probabilistic analysis, the responses were mixed or inconclusive. Asked about the probabilistic risk assessment for the General Electric (GE) Advanced Boiling Water Reactor design, the GE representative told the committee that the GE analysis assumed that the software quality assurance and V&V (verification and validation) methodologies addressed the software failure issue (Simon, 1996). Thus software failures were not explicitly included in the PRA. However, it is interesting to note that the PRA for the protection and safety monitoring system of the (Westinghouse) AP600 used a software common-mode unavailability of 1.1×10^{-5} failures per demand for any particular software module, and a software common mode unavailability of 1.2×10^{-6} failures per demand for software failures that would manifest themselves across all types of software modules derived from the same basic design program in all applications (Westinghouse/ENEL, 1992).

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

As discussed in earlier chapters, the Canadian Atomic Energy Control Board (AECB) is currently formalizing an approach for software assessment in a new regulatory guide (AECB, 1996). The AECB assessment of software focuses on four aspects: review of software requirements specifications, systematic inspection of software development and implementation, review of software testing, and confirmation of software development process and management. The AECB approach requires an analysis of software criticality to assess the role of software in plant safety. A probabilistic analysis is not required since it "is difficult to produce a statistically valid set of accident conditions that a protection system must guard against. However, we maintain that usage testing can build confidence in the reliability of the software (as long as no failures occur)" (Taylor and Faya, 1995).

In the United Kingdom, Nuclear Electric is carrying out extensive dynamic testing of at least substantial portions of Sizewell-B's software as part of its safety case for the reactor's primary protection system. A quantification of the reliability was reportedly not required for licensing, but Nuclear Electric has decided to continue the testing to more accurately estimate the reliability of its software as part of its research and development activity (Marshall, 1995).

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

In other safety-critical industries, the use of deterministic safety analysis methods is prevalent; the use of probabilistic analysis is mixed. The Federal Aviation Administration relies heavily on the use of the DO-178B standard for software quality assurance (Software Considerations in Airborne Systems and Equipment Certification) and eschews the use of a probabilistic assessment of software failure. A representative from a developer of railway control systems reported to the committee on the use of formal methods in his industry for safety assessment (requirements analysis, hazard analysis, failure modes and effects analysis), abstract modeling (Petri nets, VHDL simulations, Markov models) and detailed experimental fault injection (Profetta, 1996). Within the rail industry there is a trend towards the use of a PRA-based analysis, raising for that industry many of the same issues facing the nuclear industry. The manager of software engineering at a developer of implantable devices for cardiac rhythm management described his company's system development process, which included safety and reliability assessment and V&V at each stage (Elliott, 1996). Specification analysis included data flow diagrams, state charts, and other formal methods. Quantitative analysis included extensive use of field data and an assessment of the importance of software failure to overall system safety.

ANALYSIS

Techniques for deterministic analysis of safety and reliability are well accepted and are applicable to digital systems. Formal methods are not currently used widely but offer a good basis for safety analysis of digital systems (Leveson, 1995; Rushby, 1995).

When considering a probabilistic analysis of a system containing digital components, there are basically three choices available to the analyst. First, one can estimate a probability of failure for the digital system, including software, using the best known data and the results of statistically meaningful random tests. An uncertainty analysis can help to minimize the dependence on an uncertain input for the achievement of a reliability or safety goal. The second available choice is to assume that either the software does not fail or that it always fails. This first assumption (that it does not fail) is the assumption that coincides with not including the software in the fault tree. Alternatively, one could assume that the software will certainly fail, assign a probability of one, and design the system to survive such a failure. Many analysts, who are hesitant to model software probabilistically, leave the software out of the fault tree. Since this omission is equivalent to assuming that the software does not fail, the result may be unduly optimistic. However, if the analyst can subjectively determine a reasonable upper bound on the probability of failure (i.e., by the use of quality assurance techniques and statistically meaningful random testing), the resulting analysis may be more meaningful. The third choice is to abandon the use of probabilistic analysis for reliability and safety of a nuclear power plant entirely. This third choice seems impractical, as a PRA is a key component of nuclear power plant safety analysis and has been used effectively.

However, if traditional fault tree analysis is used in PRA, it must be recognized that it is limited in its ability to model some of the failure modes associated with digital systems, especially those that incorporate fault tolerance. There are also other methods available. For example, Markov methods are generally accepted as an appropriate method for analyzing fault-tolerant digital systems (Johnson, 1989), and some mention of Markov models has appeared in the nuclear literature (Bechta Dugan et al., 1993; Sudduth, 1993). But their use appears limited within the nuclear community. Although Markov models are more flexible than fault tree models and are useful for modeling various sequence dependencies, common-cause failures, and failure event correlations, they have the disadvantage of being hard to specify and requiring very long solution times for large models.

Recent work (Bechta Dugan et al., 1992) has expanded the applicability of fault tree models to adequately handle the complexities associated with the analysis of fault-tolerant systems without necessitating the specification of a complex Markov model. This dynamic fault tree model integrates well with a traditional fault tree analysis of other parts of the system (Pullum and Bechta Dugan, 1996). In addition to the extensions of the fault tree model, other analysis techniques have been proposed, for example, dynamic flow graphs (Garrett et al., 1995; USNRC, 1996a).

Further, fault-tolerant digital systems are known to be susceptible to "coverage failures," which are a type of common-cause failure that can bring down the entire system on a single failure. Coverage failures have been shown to dramatically affect the reliability analysis of highly reliable systems (Arnold, 1973; Bechta Dugan and Trivedi, 1989; Bouricius et al., 1969) and so it is important to include them in a model. Paula (1993) provides data for coverage failures in PLC systems used in the chemical process and nuclear power industries.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. Deterministic assessment methodologies, including design basis accident analysis, hazard analysis, and other formal analysis procedures, are applicable to digital systems.

Conclusion 2. There is controversy within the software engineering community as to whether an accurate failure probability can be assessed for software or even whether software fails randomly. However, the committee agreed that a software failure probability can be used for the purposes of performing probabilistic risk assessment (PRA) in order to determine the relative influence of digital system failure on the overall system. Explicitly including software failures in a PRA for a nuclear power plant is preferable to the alternative of ignoring software failures.

Conclusion 3. The assignment of probabilities of failure for software (and more generally for digital systems) is not substantially different from the handling of many of the probabilities for rare events. A good software quality assurance methodology is a prerequisite to providing a basis for the generation of bounded estimates for software failure probability. Within the PRA, uncertainty and sensitivity analysis can help the analyst assure that the results are not unduly dependent on parameters that are uncertain. As in other PRA computations, bounded estimates for software failure probabilities can be obtained by processes that include valid random testing and expert judgment.[1]

Conclusion 4. Probabilistic analysis is theoretically applicable in the same manner to commercial off-the-shelf (COTS) equipment, but the practical application may be difficult. The difficulty arises when attempting to use field experience to assess a failure probability, in that the experience may or may not be equivalent. For programmable devices, the software failure probability may be unique for each application. However, a set of rigorous tests may still be applicable to bounding the failure probability, as with custom systems. A long history of successful field experience may be useful in eliciting expert judgment.

Recommendations

Recommendation 1. The USNRC should require that the relative influence of software failure on system reliability be included in PRAs for systems that include digital components.

Recommendation 2. The USNRC should strive to develop methods for estimating the failure probabilities of digital systems, including COTS, for use in probabilistic risk assessment. These methods should include acceptance criteria, guidelines and limitations for use, and any needed rationale and justification.[2]

Recommendation 3. The USNRC and industry should evaluate their capabilities and develop a sufficient level of expertise to understand the requirements for gaining confidence in digital implementations of system functions and the limitations of quantitative assessment.

Recommendation 4. The USNRC should consider support of programs that are aimed at developing advanced techniques for analysis of digital systems that might be used to increase confidence and reduce uncertainty in quantitative assessments.

REFERENCES

AECB (Atomic Energy Control Board, Canada). 1996. Draft Regulatory Guide C-138 Software in Protection and Control Systems. Ottawa, Ontario: AECB.

Apostolakis, G. 1990. The concept of probability in safety assessments of technological systems. Science 250(Dec. 7):1359–1364.

Arnold, T.F. 1973. The concept of coverage and its effect on the reliability model of a repairable system. IEEE Transactions on Computers (22)3:251–254.

Bechta Dugan, J., and K.S. Trivedi. 1989. Coverage modeling for dependability analysis of fault-tolerant systems. IEEE Transactions on Computers 38(6):775–787.

Bechta Dugan, J., S.J. Bavuso, and M.A. Boyd. 1992. Dynamic fault tree models for fault tolerant computer systems. IEEE Transactions on Reliability 41(3):363–377.

Bechta Dugan, J., S.J. Bavuso, and M.A. Boyd. 1993. Fault trees and Markov models for reliability analysis of fault tolerant systems. Reliability Engineering and System Safety, 39:291–307.

Bellcore. 1992. Reliability Prediction for Electronic Equipment. Report TR-NWT-000332, Issue 4, September.

Bertolino, A., and L. Strigini. 1996. On the use of testability measures for dependability assessment. IEEE Transactions on Software Engineering (22)2:97–108.

Bouricius, W.G., W.C. Carter, and P.R. Schneider. 1969. Reliability modeling techniques for self-repairing computer systems. Pp. 295–309 in Proceedings of the 24th Annual Association of Computing Machinery (ACM) National Conference, August 26-28, 1969. New York, N.Y.: ACM.

Butler, R.W., and G.B. Finelli. 1993. The infeasibility of quantifying the reliability of life-critical real-time software. IEEE Transactions on Software Engineering 19(1):3–12.

Cooke, R. 1991. Experts in Uncertainty: Opinion and Subjective Probability in Science. Oxford: Oxford University Press.

Cox, R.T. 1946. Probability, frequency and reasonable expectation. American Journal of Physics 14(1):1–13.

DOD (U.S. Department of Defense). 1991. Reliability Prediction of Electronic Equipment. Mil-Handbook-217F. New York: Griffiss Air Force Base. December, 1991.

Eckhardt, D.E., and L.D. Lee. 1985. A theoretical basis for the analysis of multiversion software subject to coincident errors. IEEE Transactions on Software Engineering 11(12):1511–1517.

[1] Committee member Nancy Leveson did not concur with this conclusion.

[2] See also Chapter 8, Dedication of Commercial Off-the-Shelf Hardware and Software.

Elliott, L. 1996. Presentation to the Committee on Applications of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., April 16.

EPRI (Electric Power Research Institute). 1992. Advanced Light Water Reactor Utility Requirements Document, Appendix A. EPRI NP-6780-L. Palo Alto, Calif.: EPRI.

Finelli, G.B. 1991. NASA software failure characterization experiments. Reliability Engineering and System Safety 32:155–169.

Garrett, C.J., S.B. Guarro, and G. Apostolakis. 1995. The dynamic flowgraph methodology for assessing the dependability of embedded software systems. IEEE Transactions on Systems, Man and Cybernetics 25(5):824–840.

Gertman, D.I., and H.S. Blackman. 1994. Human Reliability and Safety Analysis Data Handbook. New York: John Wiley and Sons.

Goel, A. 1996. Relating operational software reliability and workload: Results from an experimental study. Pp. 167–172 in Proceedings of the 1996 Annual Reliability and Maintainability Symposium, Las Vegas, Nev., January 22–25, 1996. Piscataway, N.J.: Institute of Electrical and Electronics Engineers.

IEEE (Institute of Electrical and Electronics Engineers). 1983. IEEE Guide to Collection and Presentation of Electrical, Electronic and Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations, Std 500–1984. New York: IEEE.

Johnson, B.W. 1989. Design and Analysis of Fault Tolerant Digital Systems. New York: Addison-Wesley.

Laprie, J-C. 1984. Dependability evaluation of software systems in operation. IEEE Transactions on Software Engineering 10(6):701–714.

Leemis, L.M. 1995. Reliability: Probabilistic Models and Statistical Methods. Upper Saddle River, N.J.: Prentice-Hall.

Leveson, N. 1995. Safeware: System Safety and Computers. New York: Addison-Wesley.

Littlewood, B., and D.R. Miller. 1989. Conceptual modeling of coincident failures in multiversion software. IEEE Transactions on Software Engineering 15(12):1596–1614.

Lyu, M. (ed.) 1996. Handbook of Software Reliability Engineering. New York: McGraw-Hill.

Marshall, P. 1995. NE Tries for Quantification of Software-based System. Inside NRC 17(20):9.

McCormick, N.J. 1981. Reliability and Risk Analysis. San Diego: Academic Press.

Miller, K.W., L.J. Morell, R.E. Noonan, S.K. Park, D.M. Nicol, B.W. Murrill, and J.M. Voas. 1992. Estimating the probability of failure when testing reveals no failures. IEEE Transaction on Software Engineering 18(1):33–43.

Mitchell, C.M., and K. Williams. 1993. Failure experience of programmable logic controllers used in emergency shutdown systems. Reliability Engineering and System Safety 39:329–331.

Modarres, M. 1993. What Every Engineer Should Know About Reliability and Risk Analysis. New York: Marcel Dekker.

Newman, P. 1995. NRC Takes a Chance, Turns to Risk-based Regulation. The Energy Daily 23(168):3.

NRC (National Research Council). 1994. Science and Judgment in Risk Assessment. Board on Environmental Studies and Toxicology. Washington, D.C.: National Academy Press.

Parnas, D., A.J. van Schouwen, and S.P. Kwan. 1990. Evaluation of safety-critical software. Communications of the Association of Computing Machinery (33)6:636–648.

Paula, H.M. 1993. Failure rates for programmable logic controllers. Reliability Engineering and System Safety 39:325–328.

Paula, H.M., M.W. Roberts, and R.E. Battle. 1993. Operational failure experience of fault-tolerant digital control systems. Reliability Engineering and System Safety 39:273–289.

Profetta, J. 1996. Presentation to the Committee on Applications of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., April 16.

Pullum, L.L., and J. Bechta Dugan. 1996. Fault tree models for the analysis of complex computer systems. Pp. 200–207 in Proceedings of the 1996 Annual Reliability and Maintainability Symposium. Las Vegas, Nev., January 22–25, 1996. Piscataway, N.J.: IEEE.

RAC (Reliability Analysis Center). 1995. Nonelectronic Parts Reliability Data 1995. Rome, N.Y.: Reliability Analysis Center.

Rushby, J. 1995. Formal Methods and Their Role in the Certification of Critical Systems. Technical Report CSL-95-1. Menlo Park, Calif.: SRI International. March.

Simon, B. 1996. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Irvine, Calif., February 28.

Singpurwalla, N.D. 1995. The failure rate of software: Does it exist? IEEE Transactions on Reliability 44(3):463–466.

Sudduth, A.L. 1993. Hardware aspects of safety-critical digital computer based instrumentation and control systems. NUREG/CP-0136. Pp. 81–104 in Proceedings of the Digital Systems Reliability and Nuclear Safety Workshop. U.S. Nuclear Regulatory Commission and the National Institute of Standards and Technology, September 13–14, 1993, Rockville, Md. Washington, D.C.: U.S. Government Printing Office.

Taylor, R.P., and A.J.G. Faya. 1995. Regulatory Guide for Software Assessment. Presented at 2nd COG CANDU Computer Conference, Toronto, Ontario. October.

USNRC (U.S. Nuclear Regulatory Commission). 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. NUREG-75/014. USNRC report WASH-1400, October. Washington, D.C.: USNRC.

USNRC. 1980. Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants. NUREG/CR-1362. Washington, D.C.: USNRC. March.

USNRC. 1982a. Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants. NUREG/CR-1205. Washington, D.C.: USRNC. January.

USNRC. 1982b. Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants. NUREG/CR-1363. Washington, D.C.: USNRC. October.

USNRC. 1993a. Class 1E Digital Systems Studies. NUREG/CR-6113. Washington, D.C.: USNRC.

USNRC. 1993b. Software Reliability and Safety in Nuclear Protection Systems. NUREG/CR-6101. Washington, D.C.: USNRC.

USNRC. 1995a. Presentation by USNRC staff (J. Wermeil) to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C. October.

USNRC. 1995b. Verification and Validation Guidelines for High Integrity Systems. NUREG/CR-6293. Washington, D.C.: USNRC.

USNRC. 1996a. Development of Tools for Safety Analysis of Control Software in Advanced Reactors. NUREG/CR-6465. S. Guarro, M. Yau, and M. Motamed. Washington, D.C.: USNRC. April.

USNRC. 1996b. Presentation by USNRC staff (J. Wermeil) to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., April.

Walter, C.J. 1990. Evaluation and design of an ultra-reliable distributed architecture for fault tolerance. IEEE Transactions on Reliability 39(5):492–499.

Westinghouse/ENEL. 1992. Simplified Passive Advanced Light Water Reactor Plant Program–AP600 Probabilistic Risk Assessment. DE-AC03-90SF18495. Prepared for U.S. Department of Energy (DOE) by Westinghouse/ENEL. Washington, D.C.: DOE.

7

Human Factors and Human-Machine Interfaces

INTRODUCTION

New technology such as digital instrumentation and control (I&C) systems requires careful consideration of human factors and human-machine interface issues. New technologies succeed or fail based on a designer's ability to reduce incompatibilities between the characteristics of the system and the characteristics of the people who operate, maintain, and troubleshoot it (Casey, 1993). The importance of well-designed operator interfaces for reliable human performance and nuclear safety is widely acknowledged (IAEA, 1988; Moray and Huey, 1988; O'Hara, 1994). Safety depends, in part, on the extent to which the design reduces the chances of human error and enhances the chances of error recovery or safeguards against unrecovered human errors (Woods et al., 1994).

Experience in a wide variety of systems and applications suggests that the use of computer technology, computer-based interfaces, and operator aids raises important issues related to the way humans operate, troubleshoot, and maintain these systems (Casey, 1993; Sheridan, 1992; Woods et al., 1994). This experience is true for both retrofits (e.g., replacement of plant alarm annunciators) and the design of new systems (e.g., advanced plants).

Three recent studies highlight the importance of the "human factor" when incorporating computer technology in safety-critical systems. The study (FAA, 1996) conducted by a subcommittee of the Federal Aviation Administration (FAA) found interfaces between flight crews and modern flight deck systems to be critically important in achieving the Administration's zero-accident goal. They noted, however, a wide range of shortcomings in designs, design processes, and certification processes for current and proposed systems. Two surveys categorizing failures in nuclear power plants that include digital subsystems (Lee, 1994; Ragheb, 1996) found that (a) human factors issues, including human-machine interface errors, comprised a "significant" category (Lee, 1994; Ragheb, 1996); and (b) whereas the trend in most categories was decreasing or flat over the 13-year study period, events attributable to inappropriate human actions "showed a marked increase." The latter two studies are summarized in Chapter 4 of this document.

Two human-machine interaction issues frequently arise with the introduction of computer-based technology: (a) the need to address a class of design errors that persistently occur in a wide range of safety-critical applications or recur in successive designs for the same system; and (b) how to define the role and activities of the human operator with the same level of rigor and specificity as system hardware and software. Woods and his colleagues (1994) identify classic deficiencies in the design of computer-based technologies and show how these negatively impact human cognition and behavior. These include data overload, the keyhole effect, imbalances in the workload distribution among the human and computer-based team members, mode errors, and errors due to failures in increasingly coupled systems. A design sometimes manifests clumsy automation—that is, a design in which the benefits of the automation occur during light workload times and the burdens associated with automation occur at periods of peak workload or during safety- or time-critical operations (Wiener, 1989). Woods notes that design flaws result in computer systems that are strong and silent and, thus, not good team players (Sarter and Woods, 1995).

In many applications, the role and specific functions of the human operator are not rigorously specified in the design and are considered only after the hardware, software, and human interfaces have been specified (Mitchell, 1987, 1996). Human functions are then defined by default; the operator's role is to fill the gaps created by the limitations of hardware and software subsystems. Such design, or really the lack thereof, raises the question of whether the role and functions implicitly defined for the human operator(s) are in fact able to be effectively and reliably performed by humans. For example, are displays readable? Is information readily accessible? Is information presented at a sufficiently high level of aggregation/abstraction to support timely human decision making or does information integration and extraction impose unacceptable workload on the human operator?

Human factors engineers and researchers are quick to note that these problems are *design* problems, not inherent deficiencies of the technology (Mitchell, 1987; Sheridan, 1992; Wiener, 1989; Woods, 1993). Skillful design that effectively uses emerging technology can make a system safer, more efficient, and easier to operate. If digital I&C systems are to be readily and successfully applied in nuclear power plants, however, the design and implementation must guard against common design errors and properly address the role of humans in operating and maintaining the system.

Emerging results from both the research and practitioner communities of human factors engineering provide a range of guidance, e.g., Space Station Freedom Human-Computer Interface Guidelines (NASA, 1988); Human Factors in the Design and Evaluation of Air Traffic Control Systems (Cardosi and Murphy, 1995); User Interface Guidelines for NASA Goddard Space Flight Center (NASA, 1996). The guidance is limited, however. Anthologies of guidelines primarily address low-level issues, e.g., design of knobs and dials, rather than higher-level cognitive issues that are increasingly important in computer-based applications, such as mode error or workload (Smith and Mosier, 1988). Other guidance is conceptual or formulated as features to avoid rather than characteristics that a design should embody. For example, Wiener's notion of clumsy automation suggests a way to check a design for potential problems (Wiener, 1989), whereas Billings' human-centered automation (Billings, 1991) is a timely concept that should permeate computer design. Neither concept, however, provides readily implementable design specifications. Finally, because the science and engineering basis of human factors for computer-based systems is so new, little guidance is generally applicable (Cardosi and Murphy, 1995; O'Hara, 1994). Most studies are developed and evaluated in the context of a particular application. Thus, as the nuclear industry increasingly uses digital technology, human interaction with new computer systems must be carefully designed and evaluated in the context of nuclear applications.

Statement of the Issue

At this time, there does not seem to be an agreed-upon, effective methodology for designers, owner-operators, maintainers, and regulators to assess the overall impact of computer-based, human-machine interfaces on human performance in nuclear power plants. What methodology and approach should be used to assure proper consideration of human factors and human-machine interfaces?

Control Rooms in Existing and Advanced Plants

To acquire a context for the discussion that follows, consider the photographs of nuclear power plant control rooms in Figure 7-1, with plants ranging from the 1970s through the next generation plants of the late 1990s. These photographs show a typical progression of control rooms in nuclear power plants.

In early plants, controls and displays were predominantly analog and numbered in the thousands. In advanced plants, controls and displays are predominantly digital, with a control room that can be staffed, at least theoretically, by a single operator.

The photographs illustrate two important features associated with the introduction of digital systems in nuclear power plant control rooms. First is the need, in existing plants, to address the human factors issues of mixed-technology operations. That is, it is likely that, for the foreseeable future, control rooms in existing plants will combine both analog and digital displays and controls. Safety concerns and budget constraints ensure that for existing plants, digital technology will be introduced at a slow, cautious pace. This means, however, that good engineering practice evolved in analog systems is potentially compromised by the availability of digital systems. Likewise, the power and potential of digital controls and displays may be limited by the need to integrate them into a predominantly analog environment.

The second issue concerns the tremendous flexibility that digital technology offers to designers or redesigners of operator consoles and the control room as a whole. The flexibility and power of digital technology is both an asset and a challenge (Mitchell, 1996; Woods et al., 1994). Currently, the design of human-machine interaction lacks well-defined criteria to ensure that displays and controls adequately support operator requirements and ensure system safety. For example, there are no agreed-upon measures, other than subjective introspection, to measure cognitive workload. Design guidance is predominantly offered at low levels, e.g., color, font size, ambiance (NASA, 1988; Smith and Mosier, 1988). Guidance for higher-level, cognitive issues such as ensuring that appropriate information is available, task allocation is balanced, and both operator skills and limitations are adequately addressed is either minimal, stated quite vaguely, or application-dependent.

CURRENT U.S. NUCLEAR REGULATORY COMMISSION REGULATORY POSITIONS AND PLANS

The regulatory basis for human factors and human-machine interaction in nuclear power plant control rooms is given in Title 10 CFR Part 50, Appendix A, General Design Criteria for Nuclear Power Plants (Criterion 19, Control Room), 10 CFR 50.34(f)(2)(iii), Additional TMI [Three Mile Island]-Related Requirements (on control room designs), and 10 CFR 52.47(a)(1)(ii), Contents of Applications (for standard design certification dealing with compliance with TMI requirements).

Historically and for predominantly analog nuclear power plant control rooms, the U.S. Nuclear Regulatory Commission (USNRC) staff uses Chapter 18 (Human Factors

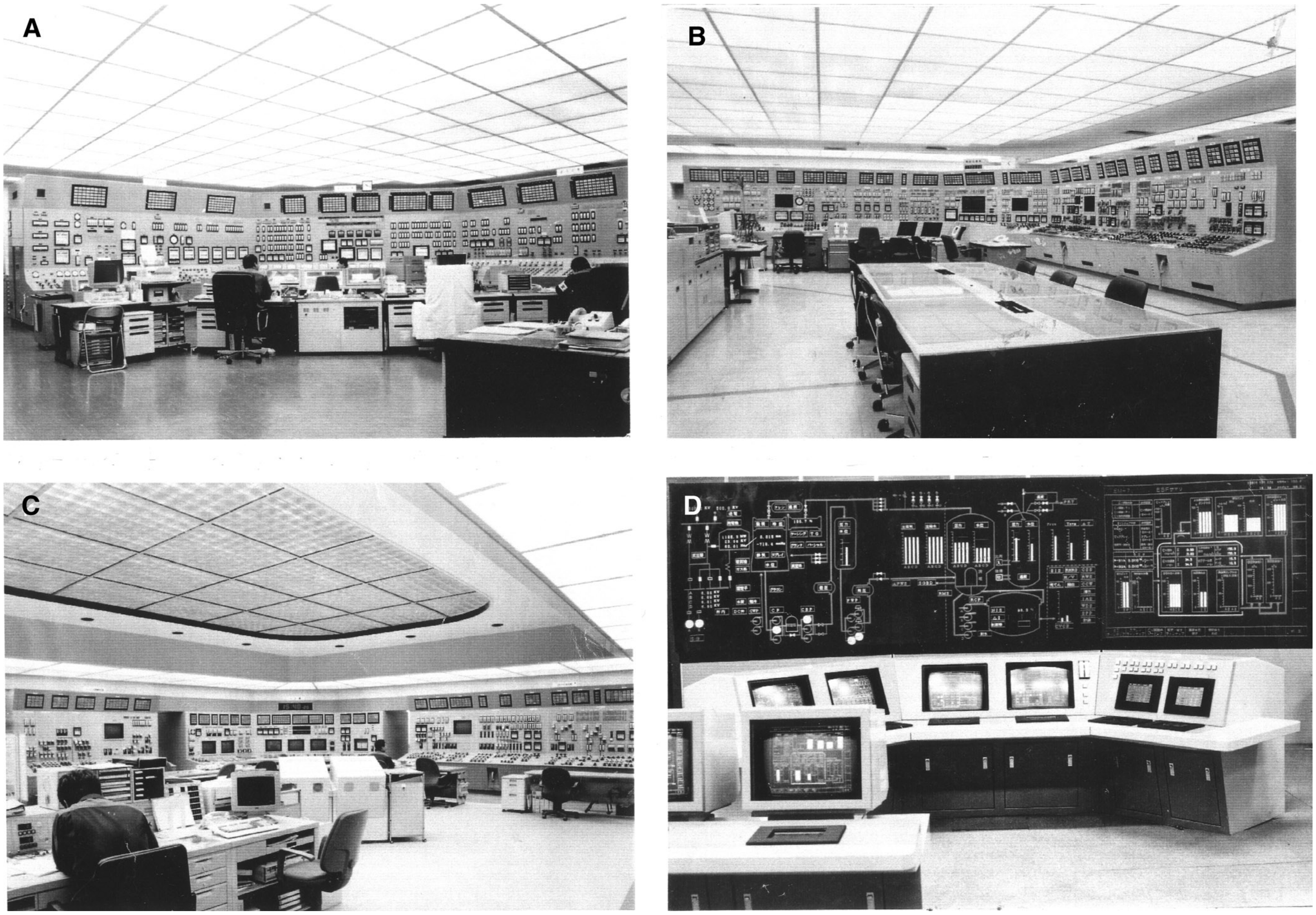

FIGURE 7-1 Evolution of Japanese nuclear power plant control rooms: (a) 1970s (Mihama-3 plant); (b) 1980s (Takahama-3 plant); (c) 1990s (Ohi-3 plant); (d) next generation plant. Source: Kansai Electric Power Co., Inc.

Engineering) of the Standard Review Plan (USNRC, 1984) and NUREG-0700, Guidelines for Control Room Design Reviews (USNRC, 1981). Both of these documents provide guidance for detailed plant design reviews. For new plants, if the design is approved and a standard design certification issued, it is expected that the implementation will conform to the specifications certified in the design review. Few changes in the control room design are expected between initial design and implementation.

In a 1993 memorandum, the USNRC Office of Nuclear Reactor Regulation communicated their 15 research needs related to human factors, five of which concerned human performance and digital instrumentation and control: (a) effects of advanced control-display interfaces on crew workload, (b) guidance and acceptance criteria for advanced human-system interfaces, (c) effect of advanced technology on current control rooms and local control stations, (d) alarm reduction, and (e) prioritization techniques and staffing levels for advanced reactors.

In 1994, the USNRC issued NUREG-0711, Human Factors Engineering Program Review Model. Recognizing the almost continuous changes in emerging human-system interface technology, the staff acknowledged that much of the human-machine interface design for advanced plants cannot be completed before the design certification is issued. Thus, the staff concluded that it was necessary to perform a human factors engineering review of the design *process*, as well as the design *product*, in advanced reactors. NUREG-0711 (USNRC, 1994) defines a program review model for human factors engineering that includes guidance for the review of planning, preliminary analyses, and verification and validation methodologies. This model is intended to be applied to advanced reactors under Title 10 CFR Part 52.

In 1995, the USNRC issued NUREG-0700 Rev. 1, Human-System Interface Design Review Guideline, as a draft report for comment (USNRC, 1995). NUREG-0700 Rev. 1 is intended to update the review guidance provided in NUREG-0700. NUREG-0700 was developed in 1981, well before many computer-based human interface technologies were widely available, and thus the USNRC staff required guidance for USNRC reviews of advanced technologies incorporated into existing control rooms. NUREG-0700 Rev. 1 has two components: a methodology that the staff may use to review an applicant's human-machine interaction design plan and a set of detailed guidelines to review a specific implementation.

Existing Plants

As indicated above, the current guidance for incorporating advanced human-system interaction technologies in existing plants is provided by NUREG-0700 Rev. 1. It should be noted that this document is a draft report for comment. NUREG-0700 Rev. 1 is intended to complement NUREG-0800. It proposes both a methodology for reviewing the process of design of the human factors elements of control rooms and specific guidelines for evaluating a design product, i.e., a specific implementation.

New Plants

NUREG-0711 specifies a program review model for advanced plants. It has two parts: (a) a general model for the review of advanced power plant human factors, and (b) specific design guidance. The guidelines are implemented in computer form, in part to facilitate updating them as state-of-the-art knowledge, human factors practice, and human-computer interaction technology evolve.

DEVELOPMENTS IN THE U.S. NUCLEAR INDUSTRY

The U.S. nuclear industry makes some use of digital technology for nonsafety systems, e.g., feedwater control, alarms, displays, and many one-for-one replacements of meters, recorders, and displays. The indication is that, as with other process control industries and most other control systems, the U.S. nuclear industry would like to make more widespread use of digital technology in a variety of applications, including safety systems.

One perceived advantage of introducing digital technology is to enhance operator effectiveness. The committee frequently heard comments suggesting that one of the biggest advantages of the introduction of digital technology was to display more information to operators and to tailor displayed information to an operator's current needs. Digital I&C makes it much easier to integrate information along with advice in a very natural way, unlike the hard-wired independent displays of the analog age. (An example of this is the cross-plot of coolant pressure and temperature on a display with both historical and predictive abilities relative to the critical criterion, the line separating liquid from gaseous state. In earlier days the human operator had to look at separate displays of temperature and pressure and then go to a chart on the wall or a nomogram to determine whether things were in a critical state.) Despite the perceived benefits, the committee also heard comments suggesting that the U.S. nuclear industry was hesitant to attempt to incorporate additional computer technology into safety-related systems owing to licensing uncertainties.

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

Foreign nuclear industries have made extensive use of digital technologies, and the control rooms of their nuclear power plants reflect extensive use of computer-based operator interfaces (White, 1994). It is important to note, however, that there are no emerging standards or sets of acceptance criteria that govern the design of human-machine interaction for such plants. For example, White (1994) notes two opposing trends in the definition of the operator's role in new advanced plant designs: in Japan and Germany, the trend is to use more automation, whereas in France the newest designs often use computer-based displays to guide plant operators.

The Halden Reactor Project of the Organization of Economic Cooperation and Development is an international effort to test and evaluate new control designs and technologies with the intent of understanding their impact on operator performance. The committee read several reports and the USNRC research staff summarized recent studies conducted by the Halden project. The committee noted that this research is very important but at this point fairly exploratory, yielding few results that can be readily used in practical power plant applications.

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

Fossil-fuel power generating plants, chemical processing, more general process control industries (e.g., textile, steel, paper), manufacturing, aerospace, aviation, and air traffic control systems all make extensive use of digital technology for operator displays, aids, and control automation. Implementation is often incremental, with improvements and refinements made gradually over the life of the design and implementation process. Some industries have developed their own industry-specific guidelines (see, e.g., Cardosi and Murphy, 1995; NASA, 1988, 1996), while others observe good human factors engineering practice.

It is important to note, however that most industries, both nuclear and nonnuclear, strongly perceive a benefit to overall system safety and effectiveness by incorporating digital technology in complex safety-critical systems. The most striking example may be in aviation. Although there are many areas that require improvement, incorporation of digital technology in commercial aircraft is widely believed to have increased overall safety and system efficiency (FAA, 1996). Reviews of cockpit automation such as those appearing in *Aviation Week and Space Technology* in the fall of 1995 note problems or "glitches" in the human interface, but none of the parties involved in the flight deck dialog (e.g., pilots, airlines, air frame manufacturers, or regulatory bodies) suggests that these glitches necessitate a return to conventional technology. The belief is that digital technology, despite problems, is often beneficial, and, with evaluation and modification, will continue to improve.

ANALYSIS

Current Situation

In many respects, the discussion in NUREG-0711 (USNRC, 1994) summarizes the current situation quite well. Consider the following excerpts:

> While the use of advanced technology is generally considered to enhance system performance, computer-based operator interfaces also have the potential to negatively affect human performance, spawn new types of human error, and reduce human reliability. . . . Despite the rapidly increasing utilization of advanced HSI technology in complex high-reliability systems such as NPP [nuclear power plants] and civilian aircraft, there is a broad consensus that the knowledge base for understanding the effects of this technology on human performance and system safety is in need of further research . . . . In the past, the [USNRC] staff has relied heavily on the use of HFE [human factors engineering] guidelines to support the identification of potential safety issues . . . . For conventional plants, the NRC HSI [human-system interaction] reviews rest heavily on an evaluation of the physical aspect of the HSI using HFE guidelines such as NUREG-0700 . . . . Relative to the guidelines available for traditional hardware interfaces, the guidelines available for software based interfaces have a considerably weaker research base and have not been well tested and validated through many years of design application . . . . [B]ecause of the nature of advanced human-system interfaces, a good system cannot be designed by guidelines alone . . . . Reviews of HSIs should extend beyond HFE guideline evaluations and should include a variety of assessment techniques, such as validations of the fully integrated systems under realistic, dynamic conditions using experienced, trained operators performing the type of tasks the HSI has been designed for. [Pp. 1-2–1-4]

Currently, and for the foreseeable future, ensuring effective design with respect to human factors of digital I&C applications cannot rest on guidelines. Guidelines are frequently well meaning but vague, e.g., "do not overload the operator with too much data." Owing to rapidly emerging computer technologies and newly conducted studies, information in guidelines is sometimes dated or obsolete. Finally, and perhaps most importantly, guidelines typically give little definitive guidance on the more serious human factors problems, e.g., cognitive workload, interacting factors in a dynamic application (O'Hara, 1994), or classic human factors issues common to many computer applications in safety-critical systems, e.g., mode error, information overload, and the keyhole effect (Woods, 1992).

In some applications (e.g., analog controls and displays), adherence to standards specified in guidelines often defines acceptance criteria for a design (O'Hara, 1994). For digital applications, however, hard, generally applicable, criteria will be a long time in coming, if they come at all. It is important to note that NUREG-0700 Rev. 1 (USNRC, 1995) does not prescribe a set of sufficient criteria for operator interfaces using advanced human-computer interaction technologies. Moreover, no other safety-critical industry has adopted well-defined or crisp criteria. Representatives of the Electric Power Research Institute told the committee, for example, that their organization had no plans to more completely formalize human factors acceptance criteria for advanced technology control rooms.

Thus, design should adhere to guidelines, where trusted guidance is available. It is necessary to go beyond guidelines, however, to ensure a safe design.

The Limits of Guidelines

As indicated in the discussion of guidelines in NUREG-0711, there are many more issues than answers in the design of computer-based operator interfaces for complex dynamic systems. Figure 7-2 depicts a hierarchy of issues related to the human factors of advanced technologies for operators of nuclear power plants. The amount of existing knowledge is inversely related to the levels of the hierarchy. Thus, the most abundant, most generally accepted, and most widely available design knowledge is for lower-level issues. Moving up the hierarchy, design knowledge is less detailed and more conceptual, and design experience is not necessarily applicable across a variety of applications (e.g., office automation to control rooms).

Human Factor Issues

Anthropometrics of Computer Workstations. At the lowest level, anthropometry—the science of establishing the proper sizes of equipment and space—there is a good deal of knowledge. Like guidelines for conventional displays and controls, the hardware associated with computer-based workstations is not subject to widespread debate. There are standards and recommendations for computer-based workstations that specify working levels, desk height, foot rests, document holders, and viewing distances (e.g., Cakir et al., 1980; Cardosi and Murphy, 1995). NUREG-0700 Rev. 1 (USNRC, 1995) includes many of these standards in its extensive section on workplace design.

Ergonomics of Displays and Controls. At the next level are issues that specify the characteristics of computer-based controls and displays. Issues include font size, use of color,

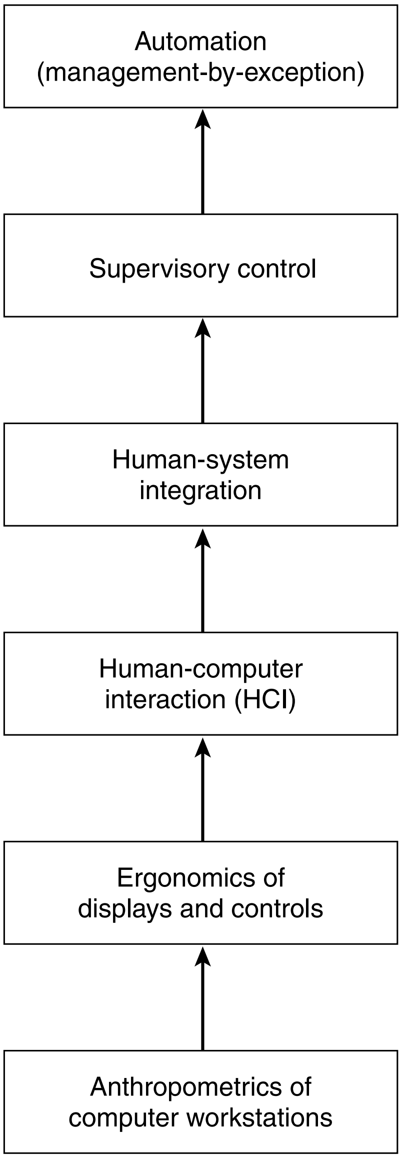
Automation (management-by-exception)
Supervisory control
Human-system integration
Human-computer interaction (HCI)
Ergonomics of displays and controls
Anthropometrics of computer workstations

FIGURE 7-2 Human factors issues in the control of safety critical systems.

input devices, and types of displays (e.g., visual, audio). Knowledge here blends commonly accepted guidelines with emerging research results that are often task- and/or user-dependent. For example, despite much dispute when first introduced in the late 1970's, a computer input device, called a mouse, was empirically shown to produce performance superior to available alternatives for pointing tasks. Today, mice are routinely packaged with computer workstation hardware. On the other hand, the number of buttons on a mouse still varies from one to three. Recommendations for the "best" design vary depending on user, task, and designer preference.

The issue of the ideal or best number of buttons on a mouse illustrates the state of a great deal of human factors engineering knowledge: there is no single, definitive best answer. In some cases, within some range, the characteristics do not make a difference and users can readily adapt to the characteristics. In other situations, an acceptable solution is task- and user-dependent. Such techniques as trial-and-error evaluations or mock-ups are needed to evaluate proposed designs. NUREG-0700 Rev. 1 contains most standard guidelines in this area.

Human-Computer Interaction. The third level, human-computer interaction, is the area to which the most study has been devoted. This area receives widespread academic and industry attention. Most guidelines address this level of human factors consideration. Issues include style of windows, windows management, dialog types, and menu styles. The guidelines address application-free, or generic, characteristics of human-computer interfaces. Most guidelines for human-computer interaction specify attributes that are *likely* to be desired, that *may* be desired, or that *must be evaluated* in the context of the application (see Cardosi and Murphy, 1995). Even at this level, there is a wide range of acceptable characteristics and no indication that a single, best design strategy is emerging. Following routine human-computer interaction style guidelines, this level of human factors issues can be adequately, though not optimally, addressed.

Combined, NUREG-0711 and NUREG-0700 Rev. 1 summarize most conventional wisdom in this area. NUREG-0711 makes a particularly important contribution with its discussion of the limitations of current guidance and state-of-the-art of design knowledge.

Human-System Integration. The transition to the fourth level of consideration, human-system integration, marks the point where many serious issues concerning human capabilities and limitations and the attributes of computer-based workstations arise. This is also the level where there are many more questions than definitive answers. At this time, the majority of issues arise, and must be addressed, in the context of the application-specific tasks for which the computer interface will be used.

Early issues, still not adequately resolved, include "getting lost" and the keyhole effect (Woods, 1984), gulfs of evaluation and execution (Hutchins et al., 1986), and the inability of designers to aggregate and abstract information meaningful to operator decision making from the vast amount of data available from control-based control systems. Essentially, issues at this level concern the semantics of the computer interface: how to design information displays and system controls that enhance human capabilities and compensate for human limitations (Rasmussen and Goodstein, 1988).

Getting lost describes the phenomenon in which a user, or operator, becomes lost in a wide and deep forest of display pages (Woods, 1984). Empirical research shows that some operators use information suboptimally in order to reduce the number of transitions among display pages

(Mitchell and Miller, 1986). When issues of across-display information processing are ignored, the computer screen becomes a serial data presentation medium in which the user has a keyhole through which data are observed. The limitations on short-term memory suggest that a keyhole view can severely limit information processing and increase cognitive workload, especially in comparison to the parallel displays common in control rooms using conventional analog technology.

Gulfs of evaluation and execution describe the conceptual distance between decisions or actions that an operator must undertake and the features of the interface that are available to carry them out. The greater the distance, the less desirable the interface (Hutchins et al., 1986; Norman, 1988). The gulfs describe attributes of a design that affect cognitive workload. The gulf of evaluation characterizes the difficulty with a particular design as a user goes from perceiving data about the system to making a situation assessment or a decision to make a change to the system. The gulf of execution characterizes the difficulty with a particular design as a user goes from forming an intention to make a change to the system to actually executing the change. Display characteristics such as data displayed at too low a level or decisions that require the operator to access several display pages sequentially, extracting and integrating data along the way, are likely to create a large gulf of evaluation. Likewise, control procedures that are sequential, complex, or require a large amount of low-level input from the operator are likely to create a large gulf of execution.

Finally, and particularly true of control rooms in which literally thousands of data items are potentially available, the issue of defining information—that is, the useful part of data—is a serious concern. The keyhole effect and getting lost are due to the vast number of display pages that result when each sensed datum is presented on one or more display pages. Rasmussen (1986) characterizes many computer-based displays provided in control rooms as representative of one-sensor/one-display design. Reminiscent of analog displays, and because displays may be used for many different purposes, data are presented at the lowest level of detail possible—typically the sensor level (Rasmussen, 1986). There is rarely an effort to analyze the information and control needs for particular operator tasks or to display information at an appropriate level of aggregation and abstraction given the current system state. Research has shown that displays tailored to operator activities based on models of the operator can significantly enhance operator performance when compared to conventional designs (e.g., Mitchell and Saisi, 1987; Thurman and Mitchell, 1995). There is no consensus, however, on the best model; see, for example, Vicente and Rasmussen (1992), who propose ecological interface design based on Rasmussen's abstraction hierarchy as an alternative to Mitchell's operator function model.

A good deal of conventional wisdom characterizing good human-system integration is available with the goal of minimizing the cognitive load associated with information extraction, decision making, and command execution in complex dynamic systems. Woods et al. (1994), for example, propose the concept of visual momentum to improve human-computer integration. Hutchins et al. (1986) use the concept of directness to bridge the gulfs of evaluation and execution, e.g., direct manipulation to support display and control. Others propose system and task models to organize, group, and integrate data items and sets of display pages (e.g., Kirlik et al., 1994; Mitchell, 1996; Vicente and Rasmussen, 1992).

Such concepts are well understood with broad agreement at the highest levels. This knowledge, however, does not, at this time, translate to definitive design guidelines or acceptance criteria. For example, there is common agreement that computer-based displays should not raise the level of required problem-solving behavior as defined by Rasmussen's SRK (skills-rules-knowledge) problem-solving paradigm (Rasmussen, 1986), yet agreement for how to design such displays does not exist. Thus, in part, design of operator workstations is an art requiring the use of current knowledge in conjunction with rigorous evaluation involving representative users and tasks.

Supervisory Control. Introduced by Sheridan (1976), the term "supervisory control" characterizes the change in an operator's role from manual controller to monitor, supervising one or more computer-based control systems. The advent of supervisory control raises many concerns about human performance. Changing the operator's role to that of a predominantly passive monitor carrying out occasional interventions is likely to tax human capabilities in an area where they are already quite weak (Wickens, 1984). Specific issues include automation complacency, out-of-the-loop familiarity, and a loss of situation awareness.

Keeping the operator in the loop has been addressed successfully by some researchers, using, for example, human-computer interaction technology to re-engage the operator in the predominantly passive monitoring and situation assessment tasks (Thurman, 1995). Most operational designs, however, address the out-of-the-loop issue by periodically requiring the operator to acknowledge the correctness of the computer's proposed solution path, despite research wisdom to the contrary (e.g., Roth et al., 1987). This design feature is similar in principle to a software-based deadman's switch: it guarantees that the operator is alive but not necessarily cognizant.

Concern about automation complacency is widespread in aviation applications where the ability of pilots to quickly detect and correct problems with computer-based navigation systems is essential for aircraft safety (Wiener, 1989). Yet, to date, there are no agreed-upon design methods to ensure that operators maintain effective vigilance over the automation or computer-based controls for which they are responsible. As with the concepts of visual momentum and direct engagement, there is widespread agreement that keeping the operator in the loop and watchful of computer-based operations is an important goal (Sheridan, 1992), but there is currently no consensus as to how to achieve it.

Over the last 20 years, as supervisory control has become the dominant paradigm, computer-based workstations have begun to incorporate a variety of operator aids, including intelligent displays, electronic checklists, and knowledge-based advisory systems. Maintaining a stable, up-to-date knowledge base about nominal and off-nominal operations to support operator decision making and problem solving is very appealing. To date, however, research has not produced designs or design methodologies that consistently live up to promised potential. For example, although some research has shown that some intelligent display designs enhance operator performance (e.g., Mitchell and Saisi, 1987; Thurman and Mitchell, 1994), other designs that sought to facilitate performance with direct perception (Kirlik et al., 1994) or direct engagement (Benson et al., 1992; Pawlowski, 1990) found that although it helped during training, the design did not enhance the performance of a trained operator.

The design of fault-tolerant systems is a comparable issue. A fault- or error-tolerant system is a system in which a computer-based aid compensates for human error (Hollnagel and Woods, 1993; Morris and Rouse, 1985; Uhrig and Carter, 1993). As with displays, there are mixed results concerning the effectiveness of specific designs. When empirically evaluated, some aids had no positive effect (e.g., Knaeuper and Morris, 1984; Zinser and Henneman, 1988); whereas some designs for operator assistants resulted in human-computer teams that were as effective as teams of two human operators (Bushman et al., 1993).

Electronic checklists or procedures for operators are another popular concept. Such checklists or procedures are technically easy to implement and reduce the overhead associated with maintaining up-to-date paper versions of procedures and checklists. The Boeing 777 flight deck includes electronic checklists and several European nuclear plants are evaluating them (Turinsky et al., 1991).

Two recent studies demonstrate the mixed results often associated with this concept. In a full motion flight simulator at NASA's Ames Research Center, a study showed that pilots made more mistakes with computer-based checklists and "smart" checklists than with conventional paper versions (Palmer and Degani, 1991). A study in a nuclear power plant control room context also had mixed results. The experiment consisted of eight teams of two licensed reactor operators (one person in each team was a senior operator) who controlled a part-task simulator called the Pressurized Water Research Facility in North Carolina State University's Department of Nuclear Engineering. The data showed that, during accident scenarios, while computer-based procedures resulted in fewer errors, time to initiate a response was significantly longer with the computer-based as compared to traditional paper-based procedures (Converse, 1995).

NUREG-0700 Rev. 1 (USNRC, 1995) devotes a section of its guidelines to analysis and decision aids. Reflecting the content of other guidelines, advice is sometimes limited or vague. For example, Guideline 5.1-6 recommends that "user-KBS [knowledge-based system] dialog should be flexible in terms of the type and sequencing of user input [p. 5-1]." Acknowledging the importance of the more general, but difficult to specify, issues, NUREG-0700 Rev. 1 includes as an appendix a list and discussion of 18 design principles. One of these general principles states that the "operator's role should consist of purposeful and meaningful tasks that enable personnel to maintain familiarity with the plant and maintain a level of workload that is not so high as to negatively affect performance, but sufficient to maintain vigilance [p. A-2]." The document notes that these principles provide the underpinning for many of the more specific guidelines contained in the body of the report.

Automation (Management-by-Exception). In the continuum from manual control to full automation the human operator is increasingly removed from system control, and in-the-loop familiarity fades. In some systems, control will be fully automatic; anomalies will cause the system to fail safe, and a human will be notified and eventually repair the automation or mitigate the problems with the controlled system. "Lights out" automation in factories and ongoing experiments in aerospace systems are current examples (Brann et al., 1996). The Airbus-A320, in which an electronic envelope overrides pilot inputs, is a step in this direction.

There are numerous human performance issues associated with fully automatic control systems in which the operator is no longer in the control loop. The current debate typically centers on how to define and design automation either for a supervisory controller or for an automation manager. Can automation in which the human is a periodic manager ever be considered human-centered automation? If so, what design characteristics must it have? Billings (1991), for example, suggests that the design must explicitly support mutual intent inferencing by both computer and human agents in order to maintain understanding on the part of the human. Or, does the design facilitate system recovery by a human engaged in fault management rather than control? NUREG-0711 acknowledges both the possibility of all of these roles for human operators in advanced control rooms and the lack of any consensus on if or how to design human interfaces to effectively support them.

Reviewing Systems for Effective Human-System Interaction

Human-system interaction reviews should proceed carefully and in a series of steps. First, guidelines, where applicable, should be consulted**.** As noted by NUREG-0711 (USNRC, 1994), however, many of the most important human performance issues associated with advanced interface technologies are not adequately covered by current guidance.

Yet to wait for the research community to derive definitive guidance would forfeit many of the advantages of emerging digital technology, both for the overall system and for the human operator. An alternative, and one pursued in almost all other industries, is to design, prototype, and evaluate candidate applications.

A review should ensure that a design is based on a detailed specification of the role and activities of the human operators. At the beginning and throughout the design process, a detailed specification of the functions of the human operator will help to increase confidence that the design process produces a successful product. Given the importance of the operator to system safety and effectiveness, operator functions should be as well and as rigorously specified as the hardware and software functions of the system. Cognitive models of operator functions and system representations offer one way to gather the information essential to create a design that effectively anticipates operator requirements, capabilities, and limitations (Hollnagel and Woods, 1983; Mitchell, 1996; Rasmussen et al., 1994). Designs based on models of human-system interaction have been empirically shown to enhance performance and reduce errors (e.g., Mitchell and Saisi, 1987; Thurman, 1995; Vicente et al., 1995).

In conjunction with cognitive models of operator activities, designers need to intermittently assess proposed features of the human-system interface with respect to the set of classic design deficiencies. For example, if modes are used, does the interface give appropriate feedback to allow the operator to rapidly understand which mode is currently active? How many displayed items and separate display pages must be called and integrated to make an assessment? Is visual momentum lost? Does the organization and access to different display pages provide a keyhole through which the operator sees only part of the system, potentially overlooking an important state, state change, or trend?

Finally, proposed designs must be evaluated in a performance-based manner. Performance-based evaluations should include a realistic task environment, statistically testable performance data, and subjects who are actual users.

The decreasing cost of emerging digital technologies allows the use of part-task simulators in which high-fidelity dynamic mock-ups of a proposed design can be implemented and rigorously evaluated. Other industries make extensive use of workstation-based part-task simulators (e.g., aviation); results are found to scale quite well to the systems as a whole (e.g., Gopher et al., 1994).

The prevalence of concepts such as user-centered design (Norman, 1988) typically means that all designers know that they must involve users early in the design process. Designers often report that users are consulted at every step. Indeed, the committee heard of design evaluations in which nuclear power plant operators joined the design team to tailor display attributes for operator consoles in advanced reactors. While user input, preference, and acceptance are important issues, they do not take the place of rigorous performance-based evaluation. Empirical evaluations demonstrate repeatedly that well-intended designs and/or user preferences sometime fail to have the anticipated beneficial effects (Andre and Wickens, 1995). Particularly in areas that are changing as rapidly as that of human-computer interaction technologies, rigorous, statistical evaluations, over and above surveys of user preferences, are essential to ensure that the desired effect is in fact achieved.

The term "performance-based evaluation" is chosen to distinguish between studies of usability versus studies of utility. Usability studies are often not rigorous enough to generate behavioral data that can be analyzed statistically. Usability studies are conducted intermittently through various phases of the design process, iterating through the "design-evaluate-design loop until the planned levels [of usability] are achieved" (Preece, 1994). Usability studies are also a mechanism for soliciting user input and advice. Typically such studies are somewhat informal, and their purpose is to ensure that the interactions the designer intended can be carried out by users. Thus, usability studies attempt to answer the question: Is the design "usable" in the ways expected during the design specification? Such studies, however, do not necessarily ensure that a design is useful, i.e., an improvement over what it replaces. Particularly with new technology and new strategies for design, usability studies, as normally conducted, do not go far enough. They fail to evaluate the utility of the output of the design process—the product—to ensure, via measurable human performance, that the results make a value-added contribution to the operator interface.

Moreover, it is essential to conduct evaluations with actual users and representative tasks. Much of the knowledge in human factors is known to be applicable to only certain classes of tasks and users (Cardosi and Murphy, 1995). NUREG-0711 notes that one weakness of guideline-based design is with interacting guidelines. The only way to ensure the effectiveness of the final product is to test it for both usability and utility with actual users and in the context of realistic tasks demands.

An approach based on a combination of judicious use of guidelines, a principled design process, realistic prototypes, and performance-based evaluation is likely to produce a design product that enhances operator effectiveness and guards against common design deficiencies in computer-based interfaces.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. Digital technology offers the potential to enhance the human-machine interface and thus overall operator performance. Human factors and human-machine interfaces are well enough understood that they do not represent a major barrier to the use of digital I&C systems in nuclear power plants.

Conclusion 2. The methodology and approach adopted by the USNRC for reviewing human factors and human-machine interfaces provides an initial and acceptable first step in a review. As described in NUREG-0700 Rev. 1 and NUREG-0711, existing USNRC procedures, for both the design product and process, are consistent with those of other industries. The guidelines are based on many already available in the literature or developed by specific industries. The methodology for reviewing the design process is based on sound system engineering principles consistent with the validation and verification of effective human factors.

Conclusion 3. Adequate design must go beyond guidelines. The discussion in NUREG-0711 on advanced technology and human performance and the design principles set out in Appendix A of NUREG-0700 Rev. 1 provide a framework within which the nuclear industry can specify, prototype, and empirically evaluate a proposed design. Demonstration that a design adheres to general principles of good human-system integration and takes into account known characteristics of human performance provides a viable framework in which implementation of somewhat intangible, but important, concepts can be assessed.

Conclusion 4. There is a wide range in the type and magnitude of the digital upgrades that can be made to safety and safety-related systems. It is important for the magnitude of the human factors review and evaluation to be commensurate with the magnitude of the change. Any change, however, that affects what information the operator sees or the system's response to a control input must be empirically evaluated to ensure that the new design does not compromise human-system interaction effectiveness.

Conclusion 5. The USNRC is not sufficiently active in the public human factors forum. For example, proposed human factors procedures and policies or sponsored research, such as NUREG-0700 Rev. 1, are not regularly presented and reviewed by the more general national and international human factors communities, including such organizations as the U.S. Human Factors and Ergonomics Society, IEEE Society on Systems, Man, and Cybernetics, and the Association of Computing Machinery Special Interest Group on Computer-Human Interaction. European nuclear human factors researchers have used nuclear power plant human factors research to further a better understanding of human performance issues in both nuclear power plants and other safety-critical industries. Other safety-critical U.S. industries, such as space, aviation, and defense, participate actively, benefiting from the review and experience of others.

Recommendations

Recommendation 1. The USNRC should continue to use, where appropriate, review guidelines for both the design product and process. Care should be taken to update these instruments as knowledge and conventional wisdom evolve—in both nuclear and nonnuclear applications.

Recommendation 2. The USNRC should assure that its reviews are not limited to guidelines or checklists. Designs should be assessed with respect to (a) the operator models that underlie them, (b) ways in which the designs address classic human-system interaction design problems, and (c) performance-based evaluations. Moreover, evaluations must use representative tasks, actual system dynamics, and real operators.

Recommendation 3. The USNRC should expand its review criteria to include a catalog or listing of classic human-machine interaction deficiencies that recur in many safety-critical applications. Understanding the problems and proposed solutions in other industries is a cost-effective way to avoid repeating the mistakes of others as digital technology is introduced into safety and safety-related nuclear systems.

Recommendation 4. Complementing Recommendation 2, although human factors reviews should be undertaken seriously, e.g., in a performance-based manner with realistic conditions and operators, the magnitude and range of the review should be commensurate with the nature and magnitude of the digital change.

Recommendation 5. The USNRC and the nuclear industry at large should regularly participate in the public forum. As noted in NUREG-0711, advanced human interface technologies potentially introduce many new, and as yet unresolved, human factors issues. It is crucial that the USNRC stay abreast of current research and best practices in other industries, and contribute findings from its own applications to the research and practitioner communities at large—for both review and education. (See also Technical Infrastructure chapter for additional discussion.)

Recommendation 6. The USNRC should encourage researchers with the Halden Reactor Project to actively participate in the international research forum to both share their results and learn from the efforts of others.

Recommendation 7. As funds are available, the USNRC's Office of Nuclear Regulatory Research should support research exploring higher-level issues of human-system integration, control, and automation. Such research should include exploration, specifically for nuclear power plant applications, of design methods, such as operator models, for more effectively specifying a design. Moreover, extensive field studies should be conducted to identify nuclear-specific technology problems and to compare and contrast the experiences in nuclear application with those of other safety-critical industries. Such research will add to the catalog of recurring deficiencies and potentially link them to proposed solutions.

Recommendation 8. Complementing its own research projects, the USNRC should consider coordinating[1] a facility, perhaps with the U.S. Department of Energy, in which U.S. nuclear industries can prototype and empirically evaluate proposed designs. Inexpensive workstation technologies permit the development of high-fidelity workstation-based simulators of significant portions of control rooms. Other industries make extensive use of workstation-based part-task simulators (e.g., aviation); results are found to scale quite well to the systems as a whole.

REFERENCES

Andre, A.D., and C.D. Wickens. 1995. When Users Want What's NOT Best for Them. Ergonomics in Design, October.

Benson, C.R., T. Govindaraj, C.M. Mitchell, and S.M. Krosner. 1992. Effectiveness of direct manipulation interaction in the supervisory control of flexible manufacturing systems. Information and Decision Technologies 18:33–53.

Billings, C.E. 1991. Human-Centered Aircraft Automation: A Concept and Guidelines. Technical Memorandum No. 103885. Moffett Field, Calif.: NASA Ames Research Center.

Brann, D.M., D.A. Thurman, and C.M. Mitchell. 1996. Human interaction with lights-out automation: A field study. Pp. 276–283 in Proceedings of the 1996 3rd Symposium on Human Interaction in Complex Systems, Dayton, Ohio, August 25–28, 1996. Los Alamitos, Calif.: IEEE.

Bushman, J.B., C.M. Mitchell, P.M. Jones, and K.S. Rubin. 1993. ALLY. An operator's associate for cooperative supervisory control systems. IEEE Transactions on Systems, Man, and Cybernetics 23(1):111–128.

Cakir, A., D.J. Hart, and T.F.M. Hart. 1980. Visual Display Terminals: A Manual Covering Ergonomics, Workplace Design, Health and Safety, Task Organization. New York: John Wiley and Sons.

Cardosi, K.M., and E.D. Murphy (eds.). 1995. Human Factors in the Design and Evaluation of Air Traffic Control Systems. Springfield, Va.: National Technical Information Service.

Casey, S. 1993. Set Phasers on Stun and Other True Tales of Design, Technology, and Human Error. Santa Barbara, Calif.: Aegean Publishing.

Converse, S.A. 1995. Evaluation of the Computerized Procedures Manual II (COMPMA II). NUREG/CR-6398. Washington, D.C.: U.S. Nuclear Regulatory Commission.

FAA (Federal Aviation Administration). 1996. The Interfaces Between Flightcrews and Modern Flight Deck Systems. Washington, D.C.

Gopher, D., M. Weil, and T. Bareket. 1994. Transfer of skill from a computer game trainer to flight. Human Factors 36(3):387–405.

Hollnagel, E., and D.D. Woods. 1983. Cognitive systems engineering: New wine in new bottles. International Journal of Man-Machine Studies 18:583–600.

Hutchins, E.L., J.D. Hollan, and D.A. Norman. 1986. Direct manipulation interfaces. Pp. 87–124 in User Centered System Design, D.A. Norman and S.W. Draper (eds.). Hillsdale, N.J.: Lawrence Erlbaum Associates.

IAEA (International Atomic Energy Agency). 1988. Basic Safety Principles for Nuclear Power Plants. Safety Series No. 75-INSAG-3. Vienna, Austria: IAEA

Kirlik, A., M.F. Kossack, and R.J. Shively. 1994. Ecological Task Analysis: Supporting Skill Acquisition in Dynamic Interaction. Unpublished manuscript. Center for Human-Machine Systems Research, School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, Ga.

Knaeuper, A., and N.M. Morris. 1984. A model-based approach for on-line aiding and training in process control. Pp. 173–177 in Proceedings of the 1984 IEEE International Conference on Systems, Man, and Cybernetics, Haifax, Nova Scotia, October 10, 1984. New York: IEEE.

Lee, E.J. 1994. Computer-Based Digital System Failures. Technical Review Report AEOD/T94-03. Washington, D.C.: USNRC. July.

Mitchell, C.M. 1987. GT-MSOCC: A domain for modeling human-computer interaction and aiding decision making in supervisory control systems. IEEE Transactions on Systems, Man, and Cybernetics 17(4): 553–572.

Mitchell, C.M. 1996. GT-MSOCC: Operator models, model-based displays, and intelligent aiding. Pp. 233–293 in Human-Technology Interaction in Complex Systems, W.B. Rouse (ed.). Greenwich, Conn.: JAI Press Inc.

Mitchell, C. M., and D.L. Saisi. 1987. Use of model-based qualitative icons and adaptive windows in workstations for supervisory control systems. IEEE Transactions on Systems, Man, and Cybernetics 17(4):573–593.

Mitchell, C.M., and R.A. Miller. 1986. A discrete model of operator function: A methodology for information display design. IEEE Transactions on Systems, Man, and Cybernetics 16(3):343–357.

Moray, N., and B. Huey. 1988. Human Factors and Nuclear Safety. Washington, D.C.: National Academy Press.

Morris, N.M., and W.B. Rouse. 1985. The effects of type of knowledge upon human problem solving in a process control task. IEEE Transactions on Systems, Man, and Cybernetics 15(6):698–707.

NASA (National Aeronautics and Space Administration). 1988. Space Station Freedom Human-Computer Interface Guidelines. NASA USE-100. Washington, D.C.: NASA.

NASA. 1996. User Interface Guidelines for NASA Goddard Space Flight Center. NASA DSTL-95-033. Greenbelt, Md.: NASA.

Norman, D.A. 1988. The Psychology of Everyday Things. New York: Basics Books.

O'Hara, J.M. 1994. Advanced Human-System Interface Design Review Guideline. NUREG/CR-5908. Washington, D.C.: U.S. Nuclear Regulatory Commission.

Palmer, E.A., and A. Degani. 1991. Electronic checklists: Evaluation of two levels of automation. Pp. 178–183 (Volume 1) in Proceedings of Sixth International Symposium on Aviation Psychology, Columbus, Ohio, April 29–May 2, 1991. Columbus Ohio: Ohio State University.

Pawlowski, T.J. 1990. Design of Operator Interfaces to Support Effective Supervisory Control and to Facilitate Intent Inferencing by a Computer-based Operator's Associate. Ph.D. dissertation, School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta.

Preece, J. 1994. Human-Computer Interaction. New York: Addison-Wesley.

Ragheb, H. 1996. Operating and Maintenance Experience with Computer-Based Systems in Nuclear Power Plants. Presentation at International Workshop on Technical Support for Licensing of Computer-Based Systems Important to Safety, Munich, Germany. March.

Rasmussen, J. 1986. Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering. New York: North-Holland.

[1] The committee recognizes that the USNRC has an obligation to maintain an "arm's-length" relationship with the regulated industry; it is inappropriate for the USNRC to fund a facility to prototype and empirically evaluate proposed designs. However, the USNRC has, particularly for expensive facilities such as large thermal hydraulic test facilities, worked in creative partnerships with the Department of Energy and industry to coordinate the specification of the basic characteristics and then coordinated their use of the facility with others (on a time-share basis, for example) so that appropriate separation is maintained but all participants obtain increased payback for their own research investments. The committee suggests that the USNRC, Department of Energy, and industry coordinate their needs and research programs, for example, through common, time-share use of simulators using high-fidelity dynamic mock-ups of typical plants. The committee notes that the USNRC, Department of Energy and its contractors, and the industry all have very similar thermal-hydraulic simulators of essentially the same plants. Picking such a model on a commonly available platform, perhaps on a time-share basis, would likely be a particularly effective research tool in the human factors and human-machine interface area.

Rasmussen, J., and L.P. Goodstein. 1988. Information technology and work. Pp. 175–202 in Handbook of Human-Computer Interaction, M. Helander (ed.). New York: North-Holland.

Rasmussen, J., A.M. Pejterson, and L.P. Goodstein. 1994. Cognitive Systems Engineering. New York: John Wiley.

Roth, E.M., K.B. Bennett, and D.D. Woods. 1987. Human interaction with an "intelligent" machine. International Journal of Man-Machine Studies 27:479–526.

Sarter, N.B. and D.D. Woods. 1995. How in the world did we ever get in that mode? Mode error and awareness in supervisory control. Human Factors 37(1):5–19.

Sheridan, T.B. 1976. Toward a general model of supervisory control. Pp. 271–281 in Monitoring Behavior and Supervisory Control, T.B. Sheridan and G. Johannsen (eds.). New York: Plenum Press.

Sheridan, T.B. 1992. Telerobotics, Automation, and Human Supervisory Control. Cambridge, Mass.: The MIT Press.

Smith, S., and J. Mosier. 1988. Guidelines for Designing User Interface Software. ESD-TR-86-278. Washington, D.C.: U.S. Department of Defense.

Thurman, D.A. 1995. Improving Operator Effectiveness in Monitoring Complex Systems: A Methodology for the Design of Interactive Monitoring and Control Interfaces. Master's thesis, School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta.

Thurman, D.A., and C.M. Mitchell. 1994. A methodology for the design of interactive monitoring interfaces. Pp. 1738–1744 in Proceedings of the 1994 IEEE International Conference on Systems, Man, and Cybernetics, San Antonio, Texas, October 2–5, 1994. Piscataway, N.J.: IEEE.

Thurman, D.A., and C.M. Mitchell. 1995. A design methodology for operator displays of highly automated supervisory control systems. In Proceedings of the 6th IFAC/IFIP/IFOR/SEA Symposium on Analysis, Design, and Evaluation of Man Machine Systems, Boston, Mass., June 27–29, 1995. Tarrytown, N.Y.: Pergamon.

Turinsky, P. J., S. Baron, W.D. Burch, M.L. Corradini, G.E. Lucas, R.B. Matthews, and R.E. Uhrig. 1991. Western European Nuclear Power Generation Research and Development. FASAC Technical Assessment Report. McLean, Va.: Science Applications International Corporation.

Uhrig, R.E., and R.J. Carter. 1993. Instrumentation, Control, and Safety Systems of Canadian Nuclear Facilities. JTEC/WTEC Monograph. Baltimore, Md.: World Technology Evaluation Center, Loyola College. July.

USNRC (U.S. Nuclear Regulatory Commission). 1981. Guidelines for Control Room Design Reviews. NUREG-0700. Washington, D.C.: USNRC

USNRC. 1984. USNRC Standard Review Plan. NUREG-0800, Rev. 1. Washington, D.C.: USNRC.

USNRC. 1994. Human Factors Engineering Program Review Model. NUREG-0711. Washington, D.C.: USNRC. July.

USNRC. 1995. Human-System Interface Design Review Guideline. NUREG-0700, Rev. 1. Washington, D.C.: USNRC. February.

Vicente, K.J., and J. Rasmussen. 1992. Ecological interface design: Theoretical foundations. IEEE Transactions on Systems, Man, and Cybernetics 22(4):589–606.

Vicente, K.J., K. Christofferson, and A. Pereklita. 1995. Supporting operator problem solving through ecological interface design. IEEE Transactions on Systems, Man, and Cybernetics 25(4):529–545.

White, J.D. 1994. Comparative Assessments of Nuclear Instrumentation and Controls in the United States, Canada, Japan, Western Europe, and the Former Soviet Union. JTEC/WTEC Annual Report and Program Summary 1993/94. Baltimore, Md.: World Technology Evaluation Center, Loyola College.

Wickens, C.D. 1984. Engineering Psychology and Human Performance. Columbus, Ohio: Charles Merrill.

Wiener, E. 1989. Human Factors of Advanced Technology ("Glass Cockpit") Transport Aircraft. Tech. Rep. 117528. Moffett Field, Calif.: NASA Ames Research Center.

Woods, D.D. 1984. Visual momentum: A concept to improve the cognitive couple of person and computer. International Journal of Man-Machine Studies 21:229–244.

Woods, D.D. 1992. Are guidelines on human-computer interaction a Faustian bargain? Computer Systems Technical Group Bulletin, August, p. 2.

Woods, D.D. 1993. Cognitive systems in context. Pp. 2–9 in Cognitive Engineering in Aerospace Applications: Pilot Interaction with Cockpit Automation, N.B. Sarter and D.D. Woods (eds.). NASA Contractor Report 177617. Moffett Field, Calif.: NASA Ames Research Center.

Woods, D.D., L.J. Johannesen, R.I. Cook, and N.B. Sarter. 1994. Behind Human Error: Cognitive Systems, Computers, and Hindsight. Wright-Patterson AFB, Ohio: Crew Systems Ergonomics Information Analysis Center.

Zinser, K., and R.L. Henneman. 1988. Development and evaluation of a model of human performance in a large-scale system. IEEE Transactions on Systems, Man, and Cybernetics 8(3):367–375.

8

Dedication of Commercial Off-the-Shelf Hardware and Software

INTRODUCTION

The nuclear industry typically obtains its components from vendors who apply the set of "nuclear-grade" criteria contained in Title 10 CFR Part 50, Appendix B. However, the nuclear industry has become a rather small market, and some vendors (such as Allen-Bradley) are discontinuing their nuclear-grade line of equipment. The decreasing number of suppliers is also leading to increasing costs for nuclear-grade equipment.

Therefore, there is potential for taking advantage of the lower cost and extensive history of widely used commercial off-the-shelf (COTS) equipment if it can be shown to meet the same quality requirements. As a result, it has become common for utilities and other companies to purchase COTS or commercial-grade items[1] and then to qualify them for use in safety systems by performing a special qualification process called "dedication" to assure an equivalent level of quality as obtained for components developed and produced under the formal quality programs of Title 10 CFR Part 50, Appendix B. The utility typically does this "dedication" by specifying essential physical and performance characteristics of the item in question and then demonstrating that the item has these characteristics.

Qualification Process

For digital instrumentation and control (I&C) equipment and software developed for nuclear-grade service from the outset, the required assurance is developed by controlling and monitoring the software design and development process as well as through formal verification and validation (see Chapter 4). For commercial items, however, such processes are not generally performed with the requisite formality and documentation; and it can be difficult to go back and reperform them, particularly at an acceptable cost. Therefore, dedication of digital I&C systems is difficult insofar as it entails assuring software correctness and identifying and evaluating the failure modes with only limited knowledge and control of the software development processes.

In general, replacement commercial equipment can be used in nuclear power plant nonsafety grade applications if it meets the utility performance standards. These standards are usually satisfied by choosing proven, commercially available items that are widely used and have an acceptable performance record in similar applications. However, in applications whose performance can affect nuclear plant safety and the plant licensing basis, a higher standard must be met and the regulatory authorities must be satisfied that the performance and quality of a given item are compatible with the conditions of the license. For these applications, an agreed-upon method is needed for assessing and qualifying the items for their intended service.

Currently, dedication of COTS digital I&C systems tends to be achieved on an individual project basis by some utilities. A more well-defined and stable approach is needed. A key issue to be resolved is how to deal with the failure modes of the item, particularly unintended or unexpected results from software or hardware failures. This involves identifying the potentially damaging failure modes, assuring that these failure modes are subject to periodic or built-in testing so their occurrence is obvious to the operators, and assuring that the plant systems and the operator's procedures and training are such that the failures can be coped with. This issue makes the dedication and subsequent licensing process particularly challenging.

This issue is equally applicable to new plants or retrofits. But the issue is pressing for existing plants since there is a need for COTS digital I&C systems to replace aging and increasingly obsolete analog items.

Statement of the Issue

What methods should be agreed upon by the regulators and the licensees to evaluate and accept the use of commercial

[1] Commercial-grade items are safety-related systems, components, or parts that were not designed and manufactured under a quality assurance program which complies with Title 10 CFR Part 50, Appendix B.

off-the-shelf digital I&C systems in safety applications in nuclear power plants?

CURRENT U.S. NUCLEAR REGULATORY COMMISSION REGULATORY POSITIONS AND PLANS

Current Position

The U.S. Nuclear Regulatory Commission's (USNRC's) stated regulatory basis for addressing COTS hardware and software is rooted in the rule governing the use of commercial-grade items in general. In particular, the USNRC has issued a revised rule, Procurement of Commercial Grade Items by Nuclear Power Plant Licensees (Title 10 CFR Part 21) (USNRC, 1995b). As stated in the public announcement accompanying the rule:

> The new regulation clarifies the process for acceptance of "commercial-grade items" for safety-related applications. The process also ensures that this is done in a manner that avoids unnecessary delay and expense while maintaining an adequate level of plant safety.
>
> The regulation contains the following provisions:
> — an expanded definition of "commercial-grade items";
> — a more flexible process allowing "dedication" licensees, manufacturers, or third parties which will ensure the item will perform its intended safety function, in addition to the quality assurance programs of dedicating entities;
> — clarification that the entity performing the "dedication" is responsible for discovering and evaluating deficiencies, reporting any defects and failures to comply.

The rule includes an important caveat, potentially applicable to digital I&C hardware and software used in safety systems. That is, the final rule reflects the USNRC position that not all components can be properly dedicated after the design or manufacturing process is completed. This caveat applies to that limited class of components for which quality assurance is an integral part of the manufacturing process, so that one or more of their critical characteristics cannot be attested to after the fact. The rule does not specifically mention digital I&C components. Subsequent activities by the USNRC staff in setting up procedures to review COTS in digital I&C applications clearly indicate the USNRC expects to use the new rule for digital systems. On this basis, the caveat does not appear to be intended to disallow digital I&C COTS.

In order to provide specificity in applying the general rule, the use of digital I&C COTS is to be addressed in the revision to the Standard Review Plan (SRP) that is under way. A new branch technical position on dedication of COTS hardware and software is also currently under development. The revised SRP is expected to endorse, perhaps with some caveats or exceptions, the draft guidance provided in this area, EPRI [Electric Power Research Institute] TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications (EPRI, 1996). The USNRC participates in and follows the work of the EPRI working group on COTS that produced this guidance document. It also participates in several industry groups active in this area.

Research and Plans

The USNRC research staff indicated to the committee that they have no specific research or plans in this area except to participate in and monitor several industry working groups, to monitor any pertinent Halden Reactor Project results, and to evaluate the recommendations from the report prepared by the MITRE Corporation, High Integrity Software for Nuclear Power Plants (USNRC, 1995a). There is other work in progress at the national laboratories sponsored by the USNRC that is applicable to the COTS issue. For example, NUREG/CR-6421, A Proposed Acceptance Procedure for Commercial Off-the-Shelf (COTS) Software in Reactor Applications, was formally issued in early 1996 (USNRC, 1996). This work is being reviewed by the USNRC in developing the revised SRP and any needed branch technical positions.

DEVELOPMENTS IN THE U.S. NUCLEAR INDUSTRY

There are a number of U.S. nuclear industry groups working on COTS as applied to digital I&C applications in nuclear power plants. Most of these groups have at least informal communication and coordination since they share some of the same members and the same general goals. The activities and particular interest of each group are briefly discussed below.

Electric Power Research Institute

A nuclear industry working group sponsored by EPRI is developing an industry consensus guideline for cost-effective evaluation and acceptance of COTS digital equipment for real-time process monitoring, control, and protection (safety) applications in nuclear power plants (EPRI, 1996). This 35-member group of nuclear utilities and vendors is drawing from other safety-critical industry experience, and it hopes to obtain USNRC support and endorsement; USNRC staff members have attended meetings. The group's approach is based on the existing and widely used guideline for COTS, EPRI NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (EPRI, 1988).

The EPRI working group agreed at the outset to base its work on the use of NP-5652 because there is an extensive experience base in dedication, although very little of it to date applies to digital I&C components. As a result, the EPRI working group is trying to make clear how to apply the

NP-5652 standard to the new issues presented by digital I&C, microprocessor-based systems. For example, NP-5652 recognizes four methods for verifying critical characteristics of a commercial device: (1) special tests and inspections, (2) commercial grade survey of supplier, (3) source verification, and (4) acceptable supplier/item performance record. For many existing components such as bolts or mechanical devices, the method of inspection or testing is adequate by itself. As is discussed elsewhere in this report, however, for digital devices including software, inspection and testing of the final product is not likely to be satisfactory. The EPRI working group also recognizes this and expects that rather than depending on a single method, a combination of the four methods must be used for digital I&C COTS applications. A second-tier document will provide specific examples and more detailed "how to" guidance (see below).

The EPRI working group has issued its guidance in draft form (EPRI, 1996). This guidance currently suggests an approach that applies criteria and verification activities appropriate for (or commensurate with) the safety significance of the application. This approach is based on the same principles as have been recognized in the USNRC's Generic Letter 95-02 as well as in the USNRC rule on dedicating commercial items (USNRC, 1995) and USNRC guidance on the use of 10 CFR 50.59. That is, not all digital I&C applications warrant an exhaustive treatment of every aspect of the design, implementation, and quality assurance provisions. Rather, the dedication activities should be commensurate with the complexity and safety significance of the specific application.

Because the USNRC staff in the past has been reluctant to accept COTS for safety-grade digital I&C applications, the EPRI working group is proceeding in two steps. First, the group is developing its high-level guideline (issued in draft form, EPRI, 1996) on which to build an industry and USNRC consensus as to how the use of COTS in digital I&C safety-grade applications could be made acceptable. The final form of this high-level guideline was to be issued during 1996. Somewhat in parallel, the working group will also develop a complementary set of more detailed guidance on how to implement the guideline.

The approach of the EPRI working group compares the vendor development, integration, testing, and configuration control processes (commercial grade) with the approach in Title 10 CFR Part 50, Appendix B (nuclear grade) (see Figure 8-1). It then assesses whether other factors compensate for differences; these factors include a careful review of operating history and experience, additional verification and

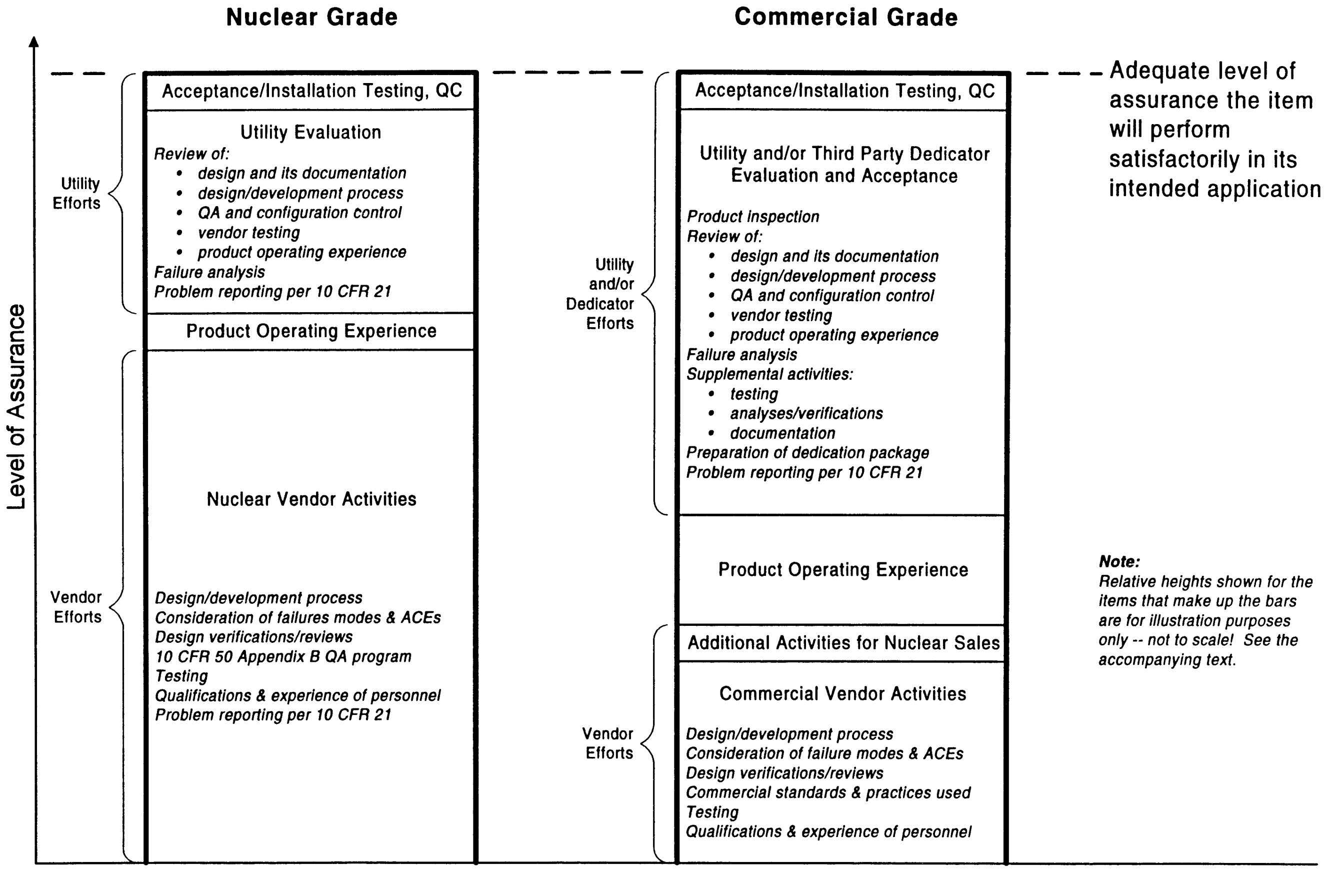
Nuclear Grade
Commercial Grade
Level of Assurance
Adequate level of assurance the item will perform satisfactorily in its intended application
Utility Efforts
Acceptance/Installation Testing, QC
Utility Evaluation
Review of:
• design and its documentation
• design/development process
• QA and configuration control
• vendor testing
• product operating experience
Failure analysis
Problem reporting per 10 CFR 21
Product Operating Experience
Vendor Efforts
Nuclear Vendor Activities
Design/development process
Consideration of failures modes & ACEs
Design verifications/reviews
10 CFR 50 Appendix B QA program
Testing
Qualifications & experience of personnel
Problem reporting per 10 CFR 21
Utility and/or Dedicator Efforts
Acceptance/Installation Testing, QC
Utility and/or Third Party Dedicator Evaluation and Acceptance
Product Inspection
Review of:
• design and its documentation
• design/development process
• QA and configuration control
• vendor testing
• product operating experience
Failure analysis
Supplemental activities:
• testing
• analyses/verifications
• documentation
Preparation of dedication package
Problem reporting per 10 CFR 21
Product Operating Experience
Additional Activities for Nuclear Sales
Vendor Efforts
Commercial Vendor Activities
Design/development process
Consideration of failure modes & ACEs
Design verifications/reviews
Commercial standards & practices used
Testing
Qualifications & experience of personnel
Note:
Relative heights shown for the items that make up the bars are for illustration purposes only -- not to scale! See the accompanying text.

FIGURE 8-1 Equivalent level of assurance for nuclear grade and commercial digital equipment. Source: EPRI.

validation, and use of special testing and (failure or hazard) analysis. The operating experience must be documented and relevant (be operated in a nearly identical application). The goal of the EPRI approach is to achieve an equivalent level of assurance for both nuclear-unique and commercial-grade, dedicated equipment.

Nuclear Utilities Software Management Group

The Nuclear Utilities Software Management Group (NUSMG) has developed Guidance for the Dedication of Commercial Grade Computer Software (NUSMG, 1995) to provide guidance on dedication of COTS software for design, maintenance, and operation of safety applications in nuclear power plants. The guideline may also be used for review of software modifications.

The NUSMG approach relies on functional requirements and acceptance criteria review, vendor survey audits, past customer surveys, similar operating history, review of software discrepancies, vendor and independent acceptance testing, and failure analysis. USNRC staff members have attended meetings of this seven-member utility group.

IEEE 7-4.3.2 Working Group

IEEE 7-4.3.2 is a principal standard for quality assurance of digital I&C systems. The standard, except for the annex, has recently been endorsed by the USNRC through issuance of Regulatory Guide 1.152. The annex to the 1993 edition of this standard (IEEE, 1993) addressed some of the technical issues associated with vendor development processes in a format similar to a typical commercial-grade survey, e.g., how the part was built, quality control methods. The standard identified specific safety requirements to test and confirm, in a manner similar to EPRI NP-5652 (EPRI, 1988).

Presently, the IEEE 7-4.3.2 working group, which consists of approximately 17 individuals from utilities, vendors, the USNRC, national laboratories, and other entities, is embarking upon a one- to two-year effort to update this standard to more fully address vendor supply, COTS, and commercial-grade dedication (Richard Blauw, working group chairman, personal communication to Tracy Wilson, March 28, 1996). The annex to the standard will also be improved to allow use of documented, relevant commercial experience—and to note its limitations. USNRC staff members have been involved in the work of this group, which has also interacted with both the EPRI and NUSMG groups described above.

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

The staff of Ontario Hydro and British Nuclear Electric have reported to the committee that they are conducting research on the use of COTS. For example, Ontario Hydro's OASES standard includes guidance on evaluation of COTS based on operating history, user input, goodness of design, software quality assurance process, and the maintenance process. A failure modes analysis may then place constraints on COTS component usage based on system design impacts, and additional verification testing and reviews may be conducted to gain additional assurance (Joannou, 1995).

While there are no current licensing limitations, the Japanese reportedly do not use COTS in safety applications, only in non-safety-related applications. However, in their latest plant designs, which are being developed with General Electric, it appears that some of the key safety-grade digital equipment and software places heavy reliance on prior satisfactory service in nonnuclear applications to establish the bases for the acceptable quality of the nuclear grade applications (Simon, 1996).

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

The EPRI working group on COTS has reportedly interacted extensively with other safety-critical industries, and the group's guidance (EPRI, 1996) is based on lessons learned from those applications. Examples known directly to the committee of COTS applications in other safety-critical industries include the new Mission Control Center at NASA's Johnson Space Center, which reported that technical and functional requirements were met at an $80 million savings by significant use of COTS hardware and software (Loral, 1996). The railroad industry is also beginning to use some COTS in switching signal designs (Profetta, 1996); but the implantable medical device sector does not yet use COTS in internal devices, although apparently it uses COTS in external devices for programming the digital circuits actually implanted (Elliott, 1996).

International Society for Measurement and Control

The SP 67 Nuclear Power Plant Standards Committee of the International Society for Measurement and Control[2] (ISA) is charged with development of standards for I&C systems in nuclear power plants and associated industries. A subcommittee of SP 67 (SP 67.16, Safety-Related, Digital-Based System Upgrades at Nuclear Power Plants) is monitoring the design, testing, installation, and licensing of analog-to-digital upgrades and the need for appropriate standards and guidelines.

One of the working groups under SP 67.16 is examining the issue of dedication of commercial-grade (COTS) hardware and software (including firmware) in nuclear safety-related control, protection, and monitoring applications (Timothy Hurst, working group chairman, personal communication to

[2] Formerly known as the Instrument Society of America.

Tracy Wilson, March 28, 1996; and working group charter). The group is considering testing, installation, operations, and configuration control aspects. The approximately 20 members of this working group represent nuclear utilities, vendors, regulators, academicians, and others.

The ISA SP 67.16 working group is interfacing with the EPRI working group (including having reciprocal members) and providing comments on the draft EPRI guidelines (EPRI, 1996). It is awaiting completion of the EPRI work before it develops its plans. The EPRI guidelines may be used to provide the basis for the development of an ISA/ANSI [American National Standards Institute] standard or guideline on COTS, although this may be several years away. USNRC staff members attend meetings of this ISA working group.

Military Uses of COTS

In 1994, the Department of Defense embarked upon an effort to reduce its reliance upon military specifications and to more fully adopt the use of COTS hardware and software. These efforts were addressed in a recent report by the Defense Science Board (1994). Also, the Canadian Department of National Defense is sponsoring research by the Canadian National Research Council on use of COTS in systems development, particularly the attendant development, deployment, and maintenance problems of integrating disparate COTS components with software extensions ("glue") (National Research Council of Canada, 1996). However, the committee is unaware of any specific guidance for evaluation of COTS that has yet resulted from these efforts.

ANALYSIS

At present there is no clear guidance for the dedication of COTS digital I&C hardware and software for safety-related application in nuclear power plants. To address this need, several industry groups are working to develop guidance documents and standards. The USNRC is participating in and monitoring the efforts of these groups with the intent of eventually endorsing the results. Such endorsement may, however, be subject to caveats or exceptions, a possibility raised by issues of consistency and efficiency: Will the eventual results produced by the different groups be consistent? Can the process be brought to closure relatively quickly so that specific, definitive regulatory guidance can be given?

With respect to the first question, contacts with the groups involved and brief reviews of the initial results, particularly EPRI TR-106439 (EPRI, 1996), indicate that there is sufficient informal coordination and communication between the various groups to allow the desired consistency to be achieved. The natural staging or sequencing of the work by the groups will also aid in achieving consistency, in that the EPRI working group's draft guidance document has already been issued, giving the other groups the benefit of the EPRI results as a guide to their own efforts. Further, the participation by USNRC staff in these working groups can also help bring consistency to these efforts.

With regard to the second question—whether the USNRC will be able to efficiently utilize the results in developing definitive regulatory guidance—the committee expects that the USNRC staff's early interaction with the working groups will put the USNRC in a position to move quickly on its formal endorsement.

An important use USNRC staff can make of its interaction with the various working groups is to review the applicable work of the national laboratories so that any differences from the evolving industry guidelines are recognized and resolved. For example, NUREG/CR-6421 (USNRC, 1996) and EPRI TR-106439 both provide suggested approaches to acceptance of COTS digital components. Differences between the two that the USNRC needs to address in developing their regulatory guidance documents include:

- The NUREG/CR-6421 approach is more detailed and relies more heavily on information extracted from existing standards. EPRI TR-106439 has less detail and counts on its second-tier "how to" guidance to provide more of this detail.
- Both documents have methods for making COTS dedication activities commensurate with safety significance. NUREG/CR-6421 considers only safety significance and largely follows the IEC 1226 standard. The EPRI approach uses both safety classification and complexity of the component.
- The two documents present their criteria in different ways, but both intend that in qualifying COTS a considerable amount of engineering judgment be applied in determining that the dedicated component meets the necessary standards. The second-tier EPRI guidance will provide examples and more explicit details as to the mechanics and specific techniques of this process.
- The NUREG report tends to be more prescriptive.

In connection with resolving these differences, the committee calls attention to the need for the COTS guidance to be clear on necessary attributes that the hardware and software must have. Once these attributes are well-defined, there may be various acceptable methods of assessing whether or not the attributes are adequately provided. These methods can include appropriate testing and experience reviews. Once these methods are defined and used, requisite experience will accumulate and provide increasing confidence. The committee notes that the FAA's DO-178B, Software Considerations in Airborne Systems and Equipment Certification (FAA, 1992), is primarily based on defining needed attributes, rather than methods of proving these attributes; the FAA document also includes guidance on assuring that these attributes are adequately satisfied by COTS. The committee suggests that the USNRC and the industry groups consider this FAA document in further work on COTS.

To summarize the committee's view of COTS, its use provides a major opportunity but also presents a challenge. The use of COTS could likely be very helpful in addressing the increasing obsolescence of installed I&C systems in nuclear plants by expanding the sources of modern equipment available for use. The challenge, particularly for safety-critical applications, is to obtain the needed quality at an acceptable cost. Dedication of commercial components requires much more information than commercial vendors are accustomed to supplying. This is because the key is assessing whether the previous applications are sufficiently similar to the application of interest and how effective the proper experience is in establishing the adequacy of important attributes such as reliability.[3] Some vendors may be unwilling to provide or share their proprietary information, particularly about development or testing procedures and results of service experience. Further, utilities and the USNRC will have to be proactive about finding ways to pool needed information, perhaps, in part, by providing and maintaining dedication on more generic components. Nevertheless, the key uncertainty is whether dedication of commercial digital I&C components will be cost-effective. Only experience will provide a definitive answer.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. Use of COTS hardware and software is an attractive possibility for the nuclear industry to pursue, provided that a technically adequate dedication process can be formulated and that this process does not negate the cost advantages of COTS.

Conclusion 2. The recently developed draft guideline of the EPRI working group, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, appears to have potential as the basis for reaching industry and USNRC consensus on the COTS issue. In view of this possibility, the committee notes that the guideline and the follow-on (second-tier) guidance should assure that the necessary and sufficient attributes of digital I&C application are defined for both hardware and software. Once these attributes are well-defined, various acceptable methods of assessing the validity of the attributes can be more readily ascertained and used and the requisite experience gained. As an example of the type of approach the committee considers appropriate, the EPRI working group and the USNRC staff should consider the FAA's DO-178B guideline for digital avionics, Software Considerations in Airborne Systems and Equipment Certification, which includes guidance on COTS.

Conclusion 3. Software quality assurance and safety and reliability assessment methods are strongly related to COTS. The committee's conclusions in Chapters 4 and 6, respectively, should therefore also be considered. Dedication processes for COTS should also prove relevant in cases where standardized software is reused among similar nuclear applications.

Conclusion 4. The USNRC involvement in the EPRI, NUSMG, IEEE, and ISA working groups is very useful and should aid the USNRC in developing specific guidance to address the COTS issue.

Conclusion 5. The approach to COTS must apply criteria and verification activities commensurate with the safety significance and complexity of a specific application. For example, the level of verification activities applied to small-scale replacements of recorders and indicators would not be the same as that applied to large-scale replacements of reactor protection systems.

Recommendations

Recommendation 1. The USNRC staff should assure that their involvement in the EPRI, NUSMG, IEEE, and ISA working groups means that USNRC concerns and positions are being addressed so that any standards or guidelines developed by these groups can be quickly accepted and endorsed by the USNRC.

Recommendation 2. The USNRC should establish what research is needed to support USNRC acceptance of COTS in safety applications in nuclear plants. This research should then be incorporated into the overall research plan.

Recommendation 3. The USNRC regulatory guidance on the use of COTS should recognize and be based on the principle that criteria and verification activities are to be commensurate with the safety significance and complexity of the specific application.

REFERENCES

Defense Science Board. 1994. Acquiring Defense Software Commercially. Washington, D.C.: Defense Science Board.

Elliott, L. 1996. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., April 16.

EPRI (Electric Power Research Institute). 1988. Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications. EPRI NP-5652. Palo Alto, Calif. EPRI.

EPRI. 1996. Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications (draft).

[3] There is controversy as to whether public domain COTS or proprietary COTS will be more acceptable. For example, some argue that proprietary COTS is more likely to be superior because the application may be more nearly similar to the intended use and there can be a more systematic collection of problems and documented resolutions. Others argue that public domain COTS, if it is properly "aged," is more reliable because it will have experienced far more different operational settings which should make it less susceptible to environmental problems. The committee does not have any information which leads to a conclusion as to which is more reliable.

EPRI TR-106439. Palo Alto, Calif.: EPRI (Also Ray Torok, EPRI, briefing to the committee, Irvine, Calif., February 28, 1996.)

FAA (Federal Aviation Administration). 1992. DO-178B, Software Considerations in Airborne Systems and Equipment Certification. Washington, D.C.: FAA.

IEEE (Institute of Electrical and Electronics Engineers). 1993. IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. IEEE Std 7-4.3.2–1993. New York.: IEEE.

Joannou, P. 1995. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., December 14.

Loral (Loral Space Information Systems). 1996. Mission Control Center Upgrade at NASA Johnson Space Center, Loral Corporation press release. Houston, Tx.

National Research Council of Canada. 1996. Project summary: Using COTS Software in Systems Development. Ottawa: National Research Council of Canada.

NUSMG (Nuclear Utilities Software Management Group). 1995. Guidance for the Dedication of Commercial Grade Computer Software (revision 5). Birdsboro, Pa.: NUSMG. January 4.

Profetta, J. 1996. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., April 16.

Simon, B. 1996. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Irvine, Calif., February 29.

USNRC (U.S. Nuclear Regulatory Commission). 1995a. High Integrity Software for Nuclear Power Plants. Report prepared by the Mitre Corporation for USNRC. NUREG/CR-6263. Washington, D.C.: USNRC.

USNRC. 1995b. Procurement of Commercial Grade Items by Nuclear Power Plant Licensees. Title 10 CFR Part 21. Washington, D.C.: USNRC.

USNRC. 1996. A Proposed Acceptance Procedure for Commercial Off-the-Shelf (COTS) Software in Reactor Applications. NUREG/CR-6421. Washington, D.C.: USNRC.

9

Case-by-Case Licensing Process

INTRODUCTION

Application of digital instrumentation and control (I&C) technology in nuclear power plants presents a licensing and regulatory challenge, for both the U.S. Nuclear Regulatory Commission (USNRC) and the industry, that in certain respects is unique. Advances in digital I&C technology can occur with such rapidity that product life cycles can often be shorter than the time required for the licensing and/or certification of the equipment for nuclear applications. For this reason, the regulatory review process must strive to keep apace of rapid advancements in digital I&C applications—applications that provide potentially significant benefits to the nuclear industry from a reliability and operational safety standpoint—while at the same time ensuring that the use of this technology is undertaken in a manner that is acceptable from a safety standpoint.

As individual utilities have sought to take advantage of the benefits of digital I&C technology, motivated in part by the increasing obsolescence of their analog systems, the USNRC has in turn endeavored to respond by developing a regulatory framework for the review and approval of such applications. To date, the regulatory review process for digital I&C upgrades has largely proceeded on a "case-by-case" basis. Individual utilities identify specific digital upgrades that they wish to make; the proposed change is evaluated pursuant to the criteria in 10 CFR 50.59 to determine whether prior regulatory approval is required; and, if such approval is required, the USNRC then undertakes a formal review of the proposed change before the change can implemented. In the event that prior USNRC review is required, the USNRC's evaluation is undertaken pursuant to broad regulatory standards that are generally applicable to the design and operation of nuclear power plants, including I&C systems, but that were not explicitly developed for digital systems.

Concerns Raised by the Case-by-Case Process

Although this case-by-case process may have certain benefits—particularly where technology is rapidly evolving and neither the industry nor the regulator has extensive experience that could, in turn, be the basis for establishing generically applicable regulatory requirements for digital upgrades—a number of concerns have been raised about this process. First, the lack of clearly defined regulatory standards for digital upgrades can make it difficult for a utility to evaluate the acceptability of a particular digital upgrade and to gauge the level of effort necessary to obtain regulatory approval. Second, the lack of such standards can lead to inconsistent regulatory reviews that are sometimes heavily influenced by the individual reviewer. As a result, requirements developed and imposed in a case-by-case context often lack the degree of rigor that would normally accompany the development of generic regulatory requirements. In other instances, the rigor of such requirements may go beyond that imposed on analog systems, even though the underlying issue appears to be no different. Third, the case-by-case approach to evaluating digital upgrades has proven to be a time-consuming and, in some cases, resource-intensive process, both for the industry and the staff. Finally, there is a concern that the USNRC has not implemented a clear, consistent policy with respect to the application of 10 CFR 50.59 to digital upgrades.

The discussion that follows examines the issue of the USNRC's regulatory process for review and approval of digital I&C upgrades.

Statement of the Issue

What changes should be considered in the regulatory process to provide more efficient and effective regulation of digital I&C systems in nuclear power plants? How can sufficient flexibility be incorporated to address the rapidly changing nature of the digital I&C technology and better match the time response of the regulatory process to the technology it controls? How can the regulatory process be made more efficient while maintaining its technical integrity?

REGULATORY FRAMEWORK FOR EVALUATING DIGITAL UPGRADES

Substantive Safety Standards

As a general rule, the USNRC applies predefined design criteria to evaluate design adequacy in the licensing and regulation of commercial nuclear power plants. These "general design criteria," which are applicable to all nuclear power plants, are codified in Appendix A of Title 10 CFR Part 50, General Design Criteria for Nuclear Power Plants. The criteria cover, among other things, the design of I&C systems in nuclear plants. The design criteria reflect the USNRC's long-standing safety philosophies of defense-in-depth and failure invulnerability.

Some aspects of the USNRC's design criteria are clear and quantitative. For example, Criterion 19, dealing with the control room, establishes the maximum radiation levels allowed for personnel in the control room. On the other hand, many design criteria are much more qualitative and general in nature. This is the case with respect to the design criteria for I&C systems. For example, Criterion 10, dealing with reactor design, states that ". . . control and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation . . . ." This, in turn, leaves considerable room for interpretation in the application of these requirements.

While the general design criteria for I&C systems are written in broadly applicable terms (i.e., the general design criteria do not refer specifically to analog or digital systems—see Criteria 2, 4, 17, 20–25), the early experience with the interpretation and application of these criteria has largely focused on analog and relay systems. Because of this, the regulatory framework for analog and relay systems has evolved and become quite refined over the years, to the point where a clear understanding exists today with regard to the applicable requirements for such systems. In recent years, however, with the move toward digital instrumentation and control systems, greater attention has focused on developing a regulatory framework for the review and approval of such systems. As discussed above, because the general design criteria for I&C systems provide high level guidance, there is considerable latitude in how these requirements are interpreted and applied. As a result, the evolution of the regulatory framework for digital I&C systems has proceeded on the above-described "case-by-case" basis, as the agency has reviewed utility-specific proposed applications of digital technology for I&C functions, without a clear view to existing regulatory guidance applied to large-scale, safety-grade systems (such as the emergency core cooling system).

Procedural Framework for Evaluating Digital Upgrades

In addition to the broad substantive standards contained in Title 10 CFR Part 50, Appendix A, the USNRC has established a process for individual utility licensees to evaluate plant-specific modifications that they may wish to make and, in particular, defining when such changes can be made without prior USNRC approval. This process, which is codified in 10 CFR 50.59 (see also discussion in Chapter 1) and covers changes in plant hardware and procedures, as well as any new plant tests or experiments, requires individual reactor licensees to assess the impact of any such proposed plant changes pursuant to several specific criteria. In pertinent part, 10 CFR 50.59 reads as follows:

> The holder of a license . . . may (i) make changes in the facility as described in the safety analysis report, (ii) make changes in the procedures as described in the safety analysis report, and (iii) conduct tests or experiments not described in the safety analysis report, without prior Commission approval, unless the proposed change, test or experiment involves a change in the technical specifications incorporated in the license or an unreviewed safety question.

This section, in turn, defines an "unreviewed safety question" as follows:

> A proposed change, test, or experiment shall be deemed to involve an unreviewed safety question (i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or (ii) if a possibility for an accident or malfunction of a different type than any previously evaluated in the safety analysis report may be created; or (iii) if the margin of safety as defined in the basis for any technical specification is reduced.

Because 10 CFR 50.59 defines the circumstances under which a utility can make a change without prior USNRC approval—and because a formal "unreviewed safety question" analysis can be an expensive and time-consuming process—this regulation plays an extremely important role and has been at the center of the discussion of how best to go about implementing digital upgrades from a procedural perspective.

In view of the importance of how 10 CFR 50.59 is interpreted and applied, and of the need for consistent and uniform application of the regulation by the industry, the Electric Power Research Institute (EPRI) and the Nuclear Management and Resources Council (NUMARC) undertook several years ago to develop an industry guidance document on the application of 10 CFR 50.59. This document, Guidelines for 10 CFR 50.59 Safety Evaluations (NSAC-125), was published in 1988 (EPRI/NUMARC, 1988). While this document has not been endorsed by USNRC, the agency has taken the position that the guidelines of NSAC-125 can be useful in the evaluation of proposed changes to the facility design or procedures, and are representative of logic used in making a 50.59 determination (USNRC, 1995).

OVERVIEW OF NUCLEAR APPLICATIONS OF DIGITAL TECHNOLOGY

Digital technology has been used in limited nuclear applications for more than 20 years, and a substantial body of industry and regulatory guidance has been developed over this period of time to support such uses. While such applications included both nonsafety functions (e.g., feedwater control), as well as some limited safety-related functions (e.g., core protection calculators, radiation monitors, and emergency load sequencers), they did not until recently make major inroads into the reactor protection systems (RPS) or the engineered safety features actuation systems (ESFAS), systems that are central to the safe operation of a nuclear facility.

With the advances in microprocessor-based digital technology, the industry expressed a growing interest in extending the benefits of digital technology beyond the traditional applications. This was driven, in part, by the realization that, as the larger I&C community was moving away from analog toward digital systems, the nuclear industry would have an increasingly difficult time servicing and replacing analog systems. But beyond this, there was a desire to take advantage of the benefits offered by digital systems from a reliability and safety standpoint. For example, the use of microprocessor-based digital technology for feedwater control (a nonsafety system) could lead to a significant reduction in plant trips, providing a clear safety and reliability advantage.

In response to this interest, several vendors undertook to develop special product lines, with a particular focus on developing digital RPS systems, working closely with individual utilities and the USNRC to obtain regulatory approval. Several individual utilities, in turn, embarked upon efforts to upgrade their existing analog RPS systems.

REGULATORY RESPONSE

Haddam Neck and the Draft Generic Letter

One of the first utilities to seek to implement a digital RPS upgrade was the Connecticut Yankee Atomic Power Company when, in 1987, the utility proposed to upgrade portions of the RPS for its Haddam Neck station. The upgrade was the first RPS upgrade to be attempted by a utility under the provisions of 10 CFR 50.59.

The proposed upgrade was to take place in two phases (Phase II would have added substantially more new microprocessor equipment than Phase I). Pursuant to the requirements of 10 CFR 50.59, the utility conducted an evaluation of both phases of the upgrade to determine whether the modification involved an unreviewed safety question (USQ) or necessitated a change in the plant's technical specifications. Based upon this evaluation, the utility concluded that, because the upgrade was essentially a replacement-in-functional-kind of RPS control system analog modules with modern microprocessor-based modules, the proposed upgrade posed no unreviewed safety questions. Accordingly, the utility proceeded with installation of Phase I of the upgrade during its 1987 refueling outage. Subsequently, given the USNRC's concern over the use of licensee-configurable, microprocessor-based, protection and control system modules, the USNRC decided to review the utility's 10 CFR 50.59 determination with regard to the already implemented Phase I of the upgrade, as well as the proposed Phase II. As a result of this review, the USNRC prepared a formal safety evaluation report (SER), a step normally undertaken only when prior regulatory approval is required. In its review, the staff reached the following conclusion (USNRC, 1990):

> The NRC staff concludes that the Phase I RPS modification is acceptable except that [Connecticut Yankee] has not demonstrated that the electrical environment of the new equipment is enveloped by the vendor's qualification testing. Because Phase II will be complete before start-up for Cycle 16 and will add substantially more new microprocessor equipment, the NRC staff requires that CYAPO [Connecticut Yankee Atomic Power Company] submit a program plan prior to restart describing the analysis, testing and schedule to resolve this concern.

The staff went on to state as follows:

> The licensee has demonstrated that the equipment is functionally a one-for-one replacement and does not result in a significant system level change[;] however, the staff considers that the differences in technology inherent in the new software controlled system present the possibilities for equipment malfunctions of a different type than previously evaluated. Malfunctions of a different type than previously evaluated in equipment important to safety is an unreviewed safety question. Digital microprocessors can malfunction in a different manner than the installed analog systems RPS and should not be installed via 10 CFR 50.59. Because several utilities have changed or are considering changing their analog systems with digital systems, the staff is considering the issuance of additional guidance to the industry addressing the 50.59 issue for replacement of analog with digital equipment.

In response to the issues raised concerning the Haddam Neck upgrade and the utility's interpretation of 10 CFR 50.59, as well as in view of the rapidly expanding interest in the utility industry in implementing digital upgrades in safety systems and a broader concern with failures of digital systems that were occurring in both nuclear and nonnuclear applications, the USNRC in August 1992 issued a draft generic letter in which it addressed the application of 50.59 to digital upgrades. In pertinent part, the draft generic letter reads as follows (USNRC, 1992):

> [T]he installation of digital based safety systems (1) is an unreviewed safety question (USQ), (2) will require review by the NRC staff, and (3) cannot be performed under the 10 CFR 50.59 rule. The Staff's position applies to all safety-related digital equipment that uses software and in particular to microprocessor based systems.

For its basis, the staff noted:

> Digital electronic equipment has different failure mechanisms and resulting system malfunctions than the existing analog systems. Some of these failure modes and system malfunctions were either not considered as part of the initial plant design (the technology did not exist, therefore, the potential malfunctions were not considered) or may not have been evaluated in sufficient detail to support the new digital systems. Since licensees are installing digital equipment in primary safety systems such as reactor protection systems, engineered safety features systems, emergency diesel generator control systems, and pump control systems, the result could be safety system failures, and/or delays in actuation, and/or unplanned plant responses. [Garten, 1992]

The effect of the draft generic letter was immediate and significant. First, it explicitly required that all safety-related digital upgrades be approved in advance by the staff, irrespective of the results of a utility's evaluation under 10 CFR 50.59. In so doing, the draft generic letter, in effect, carved out an exception to 10 CFR 50.59 for digital upgrades. Second, it caused a great deal of uncertainty among those utilities that were proceeding with digital upgrades. The utilities began to see the regulatory process governing digital upgrades as ill-defined, inconsistent, and unpredictable. Prior USNRC approval for digital upgrades was now required; and the lack of generically applicable regulatory criteria resulted in digital upgrades' being judged on a case-by-case basis. For these reasons, several utilities elected to postpone planned digital upgrades or to go forward with analog replacements as an alternative.

Industry Guidance Document and USNRC's Response

Because of the uncertainty attending digital upgrades as a result of the draft generic letter (USNRC, 1992), the industry (through EPRI and NUMARC) sought to develop more specific guidance addressing the applicability of 10 CFR 50.59 to digital upgrades, particularly with regard to safety systems, supplementing the more general guidance on 10 CFR 50.59 contained in NSAC-125 (EPRI/NUMARC, 1988). With the initiation of this effort, the USNRC withdrew the draft generic letter of August 1992.

The industry guidance document, NUMARC/EPRI TR-102348, was published in December 1993 (EPRI, 1993) and a workshop was held on its implementation in June 1994. In April 1995, the USNRC published Generic Letter 95-02 (USNRC, 1995), which generally endorsed the approach taken in EPRI TR-102348, but with two exceptions. First, the USNRC took the position that in evaluating whether an analog-to-digital upgrade may create "a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report," the "system-level" to be considered should be the digital system being installed. Second, the USNRC stated that in preparing a written safety evaluation that provides the basis for the determination that the change, test, or experiment does not involve an unreviewed safety question, the basis for a utility's "engineering judgment and the logic used in the determination should be documented to the extent practicable."

APPROACHES TO REGULATION IN OTHER COUNTRIES

The committee reviewed the experience of several foreign countries in dealing with digital I&C upgrades in nuclear plants. Because of the particular characteristics of the U.S. regulatory system, however, it is difficult to compare the case-by-case issues that are the subject of this chapter—the 50.59 process and the applicable regulatory requirements—with the regulatory framework in other countries. As a general proposition, however, the committee did find that in all instances, the safety authority undertook reviews similar in rigor to those undertaken in the United States and focused largely on the same issues, including software-induced common-mode failure with which the regulators in the United States were concerned.

RESEARCH AND PLANS

The issues associated with the case-by-case regulatory approval process are largely issues of process and policy and are not issues on which the USNRC normally conducts research. Nevertheless, there may be an important role for research with respect to the public policy impacts of the USNRC's regulatory requirements and process.

ANALYSIS

The issue of case-by-case licensing involves two fundamental questions: (1) What are the substantive regulatory standards that apply to digital upgrades and can standards be developed to provide a consistent and coherent regulatory framework for evaluating digital upgrades? (2) Under what circumstances should individual utilities be allowed to proceed with digital upgrades without advance USNRC review and approval? These two questions are discussed in turn below.

Substantive Regulatory Standards

The USNRC has maintained that digital upgrades, particularly those involving substantial safety system electronics, must be evaluated with great care, given the important role that such systems will play in plant operations and the resulting consequences if such systems fail to perform their functions properly. The USNRC points to several notable examples of such failures. These include a software error at the Bruce Unit 4 facility in Canada that resulted in a loss-of-coolant accident and minor off-site releases; software surveillance errors at the Sequoyah facility in Tennessee that had a common-mode effect; and errors in the software involving an incorrect adjustment range in the flux incore/excore calibration factor at the Turkey Point facility in Florida. In this regard, the committee heard from several utility representatives who attested to the value that the USNRC regulatory review process brought to individual upgrade initiatives. Issues were identified and solutions found, particularly where early, proactive interaction between the utility and the USNRC took place.

But, as discussed in the introduction to this chapter, there is also a concern that the regulatory review process for digital upgrades has proceeded largely on an ad hoc basis, with individual utility initiatives serving as the vehicle for fashioning a regulatory framework. Moreover, while several individual guidance documents exist (see, e.g., Regulatory Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants; ANSI/IEEE/ANS 7-4.3.2–1982, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations; ANSI/IEEE 1012–1986, IEEE Standard for Software Verification and Validation Plans; and ASME NQA-2A–1990, Part 2.7, Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications, American Society of Mechanical Engineers), there is no comprehensive body of regulatory requirements and guidance to guide the utility applicant or the USNRC reviewer.

The committee recognizes that where a first-of-a-kind application of a particular technology in a nuclear plant is proposed, it would be unreasonable to expect the USNRC to have in place a comprehensive, well-developed generic regulatory framework within which to undertake an evaluation of the proposal. Indeed, there is merit to the argument that early on in the consideration of such proposals, the case-by-case approach can be an effective means for gaining experience with the issues that must be addressed, as well as to fashion a sensible, informed regulatory framework (this has been referred to by some as the so-called "revealed standard" approach).

The risks that attend such an approach, however, include the potential for inconsistent results from case to case (based, at least in part, on the qualifications and perspective of the individual reviewers that might be involved); the possibility that, as individual reviews are undertaken, increasingly stringent requirements will be imposed over time; and an unpredictable or disproportionate commitment of resources, by both the utility and the applicant, to support the extensive interactions necessary to support such customized reviews.

As discussed in Chapter 1, in an effort to address these criticisms, the USNRC has a process under way to systematically review its internal directives and guidelines governing reviews of I&C systems with a view to adapting them for digital I&C technology (Wermiel, 1995). To be completed in mid-1997, this process involves developing a Standard Review Plan for digital upgrades to safety-related systems.

Process for Implementing Digital Upgrades

As discussed above, USNRC has established a process according to which utilities can evaluate when plant modifications can be made without prior approval. This process, set forth in 10 CFR 50.59, has been in place since 1961 and is well recognized as an essential component of the regulatory process. As a general matter, the committee believes that the provisions of 10 CFR 50.59 provide a fundamentally sound framework for evaluation of digital upgrades by utilities, as it focuses a utility's attention on whether a proposed upgrade introduces an unreviewed safety question. Recognizing the concern that the Haddam Neck proposed upgrade (see above) generated with regard to the application of 10 CFR 50.59 to safety-significant upgrades, the committee nevertheless believes that the unilateral decision of the USNRC in the 1992 draft generic letter to deem all safety-related digital upgrades employing software as posing unreviewed safety questions was inconsistent with both the letter and the spirit of 10 CFR 50.59. By its terms, 10 CFR 50.59 calls for a licensee-specific evaluation of whether a proposed change in the facility involves an unreviewed safety question.

Beyond this, the committee notes a concern with the interpretation that the agency has taken with regard to EPRI Report TR-102348 (noted above), wherein the agency concluded that in evaluating whether an analog-to-digital upgrade may create "a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report," the "system-level" to be considered should be the digital system being installed (USNRC, 1995). This interpretation of 10 CFR 50.59, which the committee was advised is not mandated as a matter of law but instead is a matter of discretion for the USNRC to decide, appears to suggest that any new failure mode at the component level would constitute an unreviewed safety question, even though the system-level function was not affected. In this regard, the committee would be concerned with the wisdom of such an approach, if the USNRC were to apply it across the board to all digital upgrades, irrespective of their safety significance. The committee heard the USNRC further refine their interpretation of the EPRI report by restricting component-level consideration for major safety systems, such as ESFAS (Wermiel, 1996). The committee strongly endorses maintaining and formalizing the distinction between major and minor safety system upgrades containing digital technology.

Finally, the committee believes that it would be useful for the USNRC to establish a process whereby it can more formally catalogue 50.59 determinations—including instances where prior USNRC review has been found to be necessary, as well as instances where it has been found not to be required— so that licensees considering digital upgrades can have the benefit of this body of experience in evaluating specific upgrades that they might be considering. The committee believes that this would provide a measure of stability and uniformity to the application of 10 CFR 50.59.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. As a general observation, the role of the regulator in overseeing the implementation of digital upgrades can be a valuable and important one. Particularly in an area such as digital I&C systems, where the state of the art evolves rapidly and where first-of-a-kind nuclear applications are contemplated, the oversight role of the regulator can bring valuable insights to the implementation of such upgrades. Indeed, the committee found several specific examples of this happening.

Conclusion 2. Nevertheless, the committee found that the regulatory response to the development and implementation of digital I&C upgrades in nuclear plants has proceeded in a manner that resulted in some degree of confusion and uncertainty within the licensee community with regard to the applicable regulatory requirements and the procedural framework for implementing such upgrades. This uncertainty and the resultant incremental cost has been a major contributor to the reluctance on the part of utilities in proceeding with digital upgrades.

Conclusion 3. The lack of generically applicable regulatory requirements for digital upgrades has resulted in a case-by-case approach that has contributed to the confusion and uncertainty. This approach to reviews may have been necessary in the early phase of the transition to digital systems. But the USNRC now has a sufficient body of experience with safety-related digital upgrades, gained over recent years and supplemented by the extensive experience of other countries and other industries, to enable the agency to establish a generically applicable regulatory regime that would govern the review and approval of such upgrades.

Conclusion 4. The process established in 10 CFR 50.59, wherein the agency has defined those circumstances where a licensee may make a modification without prior USNRC review and approval, is fundamentally sound, necessary, and consistent with the USNRC's responsibility to protect the public health and safety. In particular, it recognizes the practical necessity for licensees to make facility modifications consistent with their facility licensing basis, without the need for prior USNRC review and approval. Moreover, the process appropriately reflects the gradation of significance in changes that might be made in a nuclear plant and the USNRC's attendant role based upon these gradations. In this regard, the committee strongly believes that it is important for the USNRC to distinguish between digital upgrades that are significant (i.e., pose unreviewed safety questions) and those that are not, and tailor the scope and depth of the regulatory review in a manner that is commensurate with this gradation.

Conclusion 5. The committee believes that defining *all* safety-related digital upgrades as resulting in an unreviewed safety question, as stated in the USNRC's draft generic letter of August 1992, is contrary to both the letter and spirit of 10 CFR 50.59.

Conclusion 6. The agency has no formal process for cataloguing determinations made under 10 CFR 50.59 with regard to digital upgrades and the bases for these determinations. Such information would assist both the USNRC and the utilities in determining whether particular upgrades pose unreviewed safety questions.

Conclusion 7. Early interaction between a utility applicant and the USNRC can be extremely helpful in identifying and fleshing out important issues. Where this "proactive" interaction has occurred, the committee found that the subsequent regulatory review was more efficient and focused, minimizing resources that would otherwise be required on the part of both the utility and the USNRC.

Recommendations

Recommendation 1. The USNRC should place a high priority on its effort to develop a generically applicable framework for the review and evaluation of digital I&C upgrades for operating reactors.

Recommendation 2. In view of the rapid evolution of digital technology, a process should be established to ensure that the regulatory framework is updated to stay abreast of new developments. To ensure that this framework takes into account the best practices in other safety-critical industries, external and public review is highly desirable.

Recommendation 3. The USNRC should consider additional ways in which the guideline development process can be accelerated and streamlined. For example, consideration could be given to establishing chartered task groups involving representatives from the USNRC, the industry, and academia. These groups would be tasked and managed on a project basis to investigate and resolve unreviewed matters of possible safety significance that arise in the development and use of digital systems.

Recommendation 4. In developing its regulatory requirements, the USNRC should ensure that where issues arise that are unique to digital systems, they are treated appropriately. On the other hand, where issues arise with regard to digital upgrades that are no different from issues posed for analog systems, such issues should be treated consistently. The opportunity (or obligation) for the USNRC to review and approve digital upgrades should not be seen as an opportunity to impose new requirements on individual licensees unless the issue is unique to the application proposed.

Recommendation 5. In view of the substantial benefits of early interaction with individual utilities considering digital upgrades, as well as the benefit of working closely with industry groups and other interested members of the public in the development of standards and guidelines, the USNRC should undertake proactive efforts to interact early and frequently with individual utilities and with industry groups and other interested members of the public. In addition, it would be of benefit for the USNRC to be familiar with the broader evolving applications of digital I&C systems in both nuclear and nonnuclear applications. This, in turn, will provide a foundation for a cooperative working relationship.

Recommendation 6. The USNRC should revisit the "systems level" issue addressed in Generic Letter 95-02 and EPRI Report TR-102348 to ensure that this position is consistent with the historical interpretation of 10 CFR 50.59. The committee strongly endorses maintaining and formalizing the distinction between major and minor safety system upgrades containing digital technology.

Recommendation 7. The USNRC should establish a process for cataloguing 50.59 evaluations of digital upgrades in some centralized fashion, so that individual utilities considering such upgrades can review and consider past 50.59 determinations regarding when a particular modification has been found to result in an unreviewed safety question.

REFERENCES

EPRI (Electric Power Research Institute). 1993. Guideline on Licensing Digital Upgrades. TR-102348. Palo Alto, Calif.: EPRI.

EPRI/NUMARC (Nuclear Management and Resources Council). 1988. Guidelines for 10 CFR 50.59 Safety Evaluations. NSAC-125. Palo Alto, Calif.: EPRI.

Garten, G. 1992. Briefing to the USNRC on draft Generic Letter Proposal for digital I&C. Washington, D.C.

USNRC (U.S. Nuclear Regulatory Commission). 1990. Safety Evaluation Report by the Office of Nuclear Reactor Regulation, Reactor Protection System Upgrade (Phase One), Connecticut Yankee Atomic Power Company, Haddam Neck Plant, Docket No. 50-213, March 21. Washington, D.C.: USNRC.

USNRC. 1992. Draft Generic Letter on digital I&C upgrades. Washington, D.C.: USNRC.

USNRC. 1995. Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-to-Digital Replacements under 10 CFR 50.59. Generic Letter 95-02. Washington, D.C.: USNRC.

Wermiel, J. 1995. Update of Instrumentation and Control System Section of the Standard Review Plan, NUREG-0800. Presentation to the Advisory Committee on Reactor Safeguards of the USNRC, Rockville, Md., April 7.

Wermiel, J. 1996. USNRC briefing to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., April.

10

Adequacy of Technical Infrastructure

INTRODUCTION

Nuclear industry licensees and the regulators have reached an accord on the application of analog instrumentation and control (I&C) technology in nuclear plants. Many of the types of concerns expressed about digital technology, such as EMI/RFI (electromagnetic/radiofrequency interference) and other environmental stressors and the human-machine interface, are applicable to analog technology as well. For handling the analog I&C issues there is a technical infrastructure in place upon which the licensees and regulators rely.

There is a continuing challenge to master the current state of technology and to prepare for changes that are coming. Application of digital I&C technology is not as mature, particularly as applied in nuclear plant safety systems where high reliability and assurance of safe performance are paramount. Further, as has been noted repeatedly in this report, advances in digital I&C technology occur frequently and are rapidly adopted in many types of industries. This problem should be a particular concern for licensees, regulators, vendors, and other ancillary bodies such as standards institutes. Unless the expertise and infrastructure are there, little progress can be made.

U.S. Nuclear Regulatory Commission Activities

Because this report is a response to a request by the U.S. Nuclear Regulatory Commission (USNRC) regarding the use of digital I&C technology in nuclear power plants, the committee paid particular attention to the USNRC activities in this regard. The committee looked for evidence of a strategic approach by the USNRC to the regulation of digital I&C introduced into nuclear power plants, expecting to see a USNRC road map for its staffing, training, and research programs to support the regulation of digital I&C. Earlier concerns expressed by the Advisory Committee on Reactor Safeguards and Nuclear Safety Research Review Committee (see Chapter 1) about the need for changes in research, staffing, and training set the stage for the committee to investigate these attributes. USNRC Chairman Jackson echoed some of these concerns when she challenged the USNRC staff to prepare, perhaps with the help of "a steering committee of senior level managers as well as technical experts" and "with greater commitment than has heretofore been the case," a regulatory framework for digital I&C (Jackson, 1995). In addition, the committee was interested in the effect on the USNRC process for assessing new technology and introducing it into the nuclear industry of such factors such as declining budgets, the general decline in the number of new technical graduates, and the availability of technical expertise.

Statement of the Issue

Does the USNRC need to make changes in its staffing, training, and research program to support its regulation of digital I&C technology in nuclear power plants? If so, what is the appropriate program for the USNRC? How should this program be structured so that it maintains its effectiveness in the face of rapidly moving and developing technology and generally declining budgets?

U.S. NUCLEAR REGULATORY COMMISSION REGULATORY POSITIONS AND PLANS

Staffing

The USNRC Office of Nuclear Reactor Regulation (NRR) is charged with all licensing and inspection activities associated with the design, construction, and operation of existing and proposed nuclear power plants. They are supported in this role by inspectors from the USNRC's regional offices and by on-site inspectors at the nuclear power plants. The USNRC Office of Nuclear Regulatory Research (RES) is tasked with providing independent information support for regulatory decision making, conducting research to resolve safety issues and to anticipate potential problems, and developing technical regulations and standards. In FY 1996, the USNRC had 10 NRR staff members and 6 RES staff members involved in digital I&C work, out of a total staff of 650 (NRR) and 212 (RES), respectively. These figures are a slight increase over the FY 1994-1995 period.

Training

In their October 1995 discussions with the committee (see Appendix B), the USNRC staff noted that they had several decades of experience with digital I&C technology. Nonetheless, the staff reported that they are improving their expertise in this area by hiring experienced personnel and improving the training of existing staff on a staff-specific basis at courses offered by universities, industry groups, and commercial companies. In FY 1996, $16,000 was allocated in the USNRC training budget for these external training courses. (In FY 1994, only $5000 was budgeted.)

A digital I&C working group is developing a training program at the USNRC Technical Training Division in Chattanooga, Tennessee, whose target audience is intended to be region-based inspectors, technical reviewers at headquarters, and resident inspectors at nuclear power plants. The program will involve commercial courses to provide a technical foundation and an annual “digital I&C regulatory perspectives” workshop to provide knowledge and skills in agency policy and inspection techniques. In FY 1996, the Technical Training Division allocated 1.5 staff members to this area, out of a total staff of 30 and a training budget of approximately $4 million. The committee was briefed twice on this training program, in April and October 1995 (see Appendix B), and discusses it again later in this chapter.

Research Plan

The RES office conducts its research (including the area of I&C technology) primarily to support user (NRR) needs, although some research is anticipatory. The NRR office also sponsors some “technical assistance” work in I&C technology, primarily at the Lawrence Livermore National Laboratory in California. The USNRC I&C research program includes work on a number of topics, including software verification and validation, high-integrity software for nuclear power plants, development of new regulatory guides, assessment of software languages, and environmental qualification of digital I&C equipment. New research needs are identified from current research work, other federal agency research work (such as at the Center for High Integrity Software Systems Assurance of the National Institute of Standards and Technology), involvement in foreign research (the Halden Reactor Project), and other safety-critical industry interactions (e.g., with the Federal Aviation Administration).

The committee noted with some concern that the RES research budget is expected to decrease by one-third during the next few years, although it is unclear how much of the reduction the digital I&C area will absorb. (Total RES funding allocated to digital I&C technology was approximately $3 million in FY 1996, a very slight increase over FY 1995, out of a total RES research budget of $68 million and NRR research budget of $14 million in FY 1996.) Budget reductions are also being faced in the coming years by the national laboratories of the Department of Energy, where much of the USNRC’s research is conducted. In an age of continuing technological evolution, reducing investment in research and development adds to the importance of making good strategic decisions.

DEVELOPMENTS IN THE U.S. NUCLEAR INDUSTRY

During the course of Phase 2 activities, the committee talked with three digital I&C vendors about their basic approach to providing digital systems to the nuclear industry: Foxboro Controls, General Electric Nuclear Engineering, and Westinghouse. The committee did not obtain specific information on their staffing, training, or research planning. The business opportunities perceived by these (and similar) companies, upon which the nuclear industry depends for digital I&C systems, undoubtedly will influence their staffing, training, and research.

The committee also talked with a number of nuclear utilities engaged in digital I&C upgrades: Baltimore Gas and Electric Company, Public Service Electric and Gas Company, Northeast Utilities, and Pacific Gas and Electric Company. Each of their approaches to staffing, training, and research appeared to be somewhat similar.

Baltimore Gas and Electric Company (Calvert Cliffs plant in Lusby, Maryland) has initiated in-house software engineering training courses with an emphasis on acquiring practical experience. In conducting upgrades, they either use in-house staff with the required expertise or hire expert consultants to assist. The representative from Public Service Electric and Gas Company (Salem plant in Salem, New Jersey) pointed out that training and staff development activities must address organizational issues that may exist within utilities. For example, utility organizations often separate instrumentation and control from computer systems, which may result in segregation of staff expertise on digital I&C technology within one part of the organization while responsibility for a digital I&C upgrade belongs to another. This hampers transfer of knowledge and expertise.

Much of the research in the U.S. nuclear industry is sponsored by organizations such as the Electric Power Research Institute (EPRI). For example, the committee notes that EPRI and the Tennessee Valley Authority have established an advanced power plant I&C center at TVA’s Kingston power plant. The center is intended to be a focal point and test bed for research on advanced I&C technologies for all power and process industries. The center will also promote technology transfer and offer technical courses. At the present time the USNRC does not participate in this endeavor.

DEVELOPMENTS IN THE FOREIGN NUCLEAR INDUSTRY

During the course of Phase 2 activities, the committee also talked with representatives from the Canadian and Japanese nuclear power industries and had access to information on the British and French experiences with digital I&C pertaining to software quality assurance. The committee did not obtain information on their staffing, training, or research plans.

The Japanese have a technical advisory committee on nuclear power generation to coordinate resolution of technical issues between licensees and the regulator, the Ministry of International Trade and Industry (MITI). A prototype qualification test of the digital safety systems for the advanced pressurized water reactor (APWR) and advanced boiling water reactor (ABWR) designs was conducted during 1987–1991 by the Nuclear Power Engineering Corporation, sponsored by MITI. The Japan Atomic Energy Research Institute will initiate a project this year to study reliability of digital I&C systems. The major Japanese nuclear vendors also have large in-house research activities, coordinated with the nuclear utilities and centered on research and development of digital systems for their advanced plants. Digital upgrades to replace obsolescent analog equipment is not a major concern in Japan (Utsumi, 1996).

DEVELOPMENTS IN OTHER SAFETY-CRITICAL INDUSTRIES

In the course of its study, the committee also talked to a number of representatives from other safety-critical industries (see Appendix B). The committee did not receive specific information about how they conducted their own staffing, training, and research programs. However, it was interesting to note similar concerns about regulator expertise in the railroad and medical sectors; representatives from both sectors felt that their industry was well ahead of the regulator in digital application expertise. In the field of aerospace, the FAA's use of designated engineering representatives to supplement its own staff levels (and expertise) was an interesting approach. The designated engineering representatives are not FAA employees but are certified by the FAA in the industry and provide expertise and oversight to assure FAA requirements are met. Based on discussions with the committee, most vendors in other industries maintain in-house advanced technology offices and conduct collaborative research externally with universities.

ANALYSIS

To establish and maintain an adequate and effective regulatory program for digital I&C technology, the USNRC needs the following: (a) sufficient numbers of staff conducting an efficient review process; (b) an introductory and continuing (advanced) training program for existing staff and a targeted digital I&C staff recruitment program that assure that all regulatory staff share a common understanding of state-of-the-art digital technology, incorporate experience from retrofit reviews, and stay abreast of new technological developments; and (c) an anticipatory, focused research program that supports regulatory needs.

Staffing

The USNRC is charged with regulating implementation of nuclear technology. However, the staff has been criticized by members of the Advisory Committee on Reactor Safeguards (see, e.g., Lewis, 1992) for not acquiring the proper level of staffing and training appropriate to the rapidly moving digital I&C technology. There are a number of factors that make it difficult to stay current in this area. Computer technology is a rapidly growing area but there is a general decline in the number of new technical graduates interested in the nuclear field. This is because the field of nuclear power is not growing. There is a lack of new power plant construction in the U.S. nuclear industry and the USNRC is faced with a declining budget. All of these factors make it more difficult to recruit the needed well-trained computer science or software engineers. The committee has been told by a number of utilities that when digital I&C retrofits require USNRC staff review, this process may typically entail an extra six months of time and significant expenditure of staff resources to respond to USNRC questions and regulatory uncertainty. These factors often persuade the utility applicant to modify (and downscale, if needed) the proposed change to allow the change to fall within the scope of 10 CFR 50.59. Such reluctance to make more complete plant modifications does not prevent maintaining plant safety; but it may mean that safety improvements are not being made and that maintaining adequate safety becomes more difficult and expensive.

If the estimates given the committee by the utilities of extra time and expense required to respond to USNRC staff reviews have widespread validity, then it must be questioned whether enough USNRC staff are being assigned to the digital I&C area or whether the USNRC's review process itself cannot be made more efficient. The USNRC organizational structure itself—with its intentional separation between the research (RES) and regulatory (NRR) offices—may be causing other problems, e.g., reduced intrastaff communication, duplication of research functions in both offices, or an overemphasis of research on near-term issues and insufficient attention to longer-range, developing needs. In short, if needed interaction or techniques are not readily available because of organizational hindrances, these hindrances may be a source of delays in the review process that must be addressed.

With respect to standards and guidance documents, the USNRC depends on industry groups and professional societies to develop them in the first instance. These standards and documents are then reviewed and endorsed by the USNRC, usually with caveats and exceptions. This process for developing standards moves slowly, taking from one to a few years, with additional time required for official USNRC review and approval (a long time cycle unsuited to keeping pace with rapid developments). Although this approach has not been adopted for the purpose of minimizing USNRC staff, possibly it is thought to be helpful in this regard. As a result, the efforts of the USNRC staff may be focused exclusively on reviewing and adopting standards for technology, leading to inefficiencies and discouraging personnel by isolating them from the mainstream of the technology.

Training

A set of minimal required technical skills for the regulation of current and future digital I&C systems can be defined. These skills would include hardware, software, the human-machine interface, digital systems design, nuclear systems, with software quality assurance techniques representing a particular training need. Emphasis should be placed on obtaining and training personnel with cross-discipline skills such as human factors knowledge combined with knowledge of digital computers, computer interfaces, and software. This defined set of skills could be used to measure the current skill levels of USNRC staff members charged with regulating digital I&C systems, and an appropriate training program could be put in place to strengthen skills where needed. If in order to meet regulatory needs a delegation system analogous to the FAA's use of designated engineering representatives is found to be needed, then a skill category for managing the delegates could be added.

At the time of the committee's spring 1995 visit to the USNRC Technical Training Center in Chattanooga, Tennessee (see Appendix B), personnel at the training center indicated that they were in fact developing a training curriculum for digital I&C technology, in spite of a general reduction in training budgets. The committee understands that since this time a training program has been initiated. A first of a projected annual series of Digital I&C Regulatory Perspectives workshops was held in December 1995 and in addition USNRC regulatory staff personnel have attended specific digital technology training courses.

Although internal assessments by the USNRC of the skills, knowledge, and aptitudes they believe are requisite for the regulation of digital I&C systems are useful, the committee believes they are not as effective as a thorough external assessment. The USNRC's new training program for digital I&C could be subjected to outside review and perhaps evaluated by independent training organizations (such as the International Society for Measurement and Control or the Institute for Nuclear Power Operations) or certification processes.

Another factor to consider in addressing staff training is significant variations that may exist among USNRC headquarters (NRR) technical reviewers of proposed upgrades and among USNRC regional inspectors in terms of technical expertise and areas of emphasis. (It may be noted that a USNRC Inspector General audit report dated December 27, 1995, found large disparities between regional inspection programs.) These differences may either slow down the review process or result in inadequate reviews.

In some disciplines (e.g., engineering, medicine), when individuals attain a defined level of competence they become "certified," "qualified," or "licensed." This entails application of standards for both a basic grasp of the current state of the art and more importantly continuing education to stay abreast of new technological developments. Formal certification of software engineers is a controversial topic but there are approaches such as the FAA's designated engineering representative program. If an outside organization (e.g., the American National Standards Institute or the Institute of Electrical and Electronics Engineers) could provide such a mechanism for USNRC staff personnel (and utility personnel), this might alleviate some of the problems of inconsistency in regulatory reviews, particularly when combined with improved and clarified regulatory criteria (see Chapter 9).

Part of the committee's consideration of USNRC professional development and training activities was the above-mentioned visit to the USNRC Technical Training Center, where a set of control room simulators representative of a few of today's plants are located. Only one of these simulators (Black Fox) represents a digital I&C based control room and it is not state-of-the-practice. The newest of the simulators is of 1971 vintage. These simulators are used to train USNRC headquarters and regional personnel as well as the resident inspectors at the individual plants, primarily through illustrating plant transient response and control room crew response and duties. There is apparently little or no focus on using the simulators to teach or illustrate the types of changes that the retrofits of digital I&C technology bring to the existing control rooms and control panels or to illustrate the issues of concern to the USNRC in regulating these changes. However, the committee notes that these simulators might be very useful in this regard. For example, the simulators could themselves be modified to reflect mixed digital- and analog-based equipment such as digital-based meters and recorders, monitors, keyboards, touch screens, and computer-based alarm systems. In this way USNRC personnel could see for themselves the impact on control room operators. Also, modifying the hardware and software and keeping them current would provide some useful practical experience.

Research Plan

The committee also examined the research program of the USNRC's Office of Nuclear Regulatory Research in the digital I&C technology area. The committee found this program to be a disjointed collection of studies, which the USNRC personnel involved in the work agreed lacks an underlying strategic plan. Although the studies under way in the USNRC research program may be able to resolve some of the issues confronting the regulators in applying digital I&C technology, a more structured, coherent, strategic plan is needed to better utilize the limited resources available and to obtain a more complete resolution of all the issues. A strategic plan would also support coordination of the USNRC program with programs of the nuclear industry and others active in the area. This problem has been identified before in reviews of the research program by the Nuclear Safety Research Review Committee (NSRRC, 1994).

Preceding chapters in the present report have identified areas where the committee believes the USNRC research could be more effective:

In Chapter 3, Systems Aspects of Digital I&C Technology, the committee recommends that the USNRC develop and provide specific guidance in digital I&C architecture including separation of protection and control functions; implementation of closed loop control algorithms so they are executed in a predictable manner; the use of mathematics to specify control and command functions for better understanding and easier review; and the handling of data bases used by command and control functions.

In Chapter 4, Software Quality Assurance, the committee recommends that USNRC research in software quality assurance focus on early phases of the software life cycle.

In Chapter 5, Common-Mode Software Failure Potential, the committee recommends the USNRC redirect research plans on common-mode software failure. Specifically, the committee suggests that funding research to try to evaluate design diversity is not a reasonable use of USNRC research funds.

In Chapter 6, Safety and Reliability Assessment Methods, the committee recommends that the USNRC research plan include quantitative assessment methodologies for the software and hardware of digital systems. Although the absolute values of quantitative assessments of software failure probabilities will have large uncertainties, the rigor and systematic approach of quantitative assessments would lead to better analyses. Also in Chapter 6, the committee recommends that the USNRC strive to develop methods to use the experiential data from COTS equipment in performing quantitative assessments.

In Chapter 7, Human Factors and Human-Machine Interfaces, the committee recommends that the USNRC research in the human factors area be leveraged with research and best practices in other industries. The committee recommends that results from the USNRC research be contributed to the research community at large to obtain the benefits of broad-based review and discussion. Further, the committee recommends that the USNRC consider supporting research at the higher levels of human-system integration. Finally, the committee recommends that the USNRC consider coordinating a facility in which the U.S. nuclear industry can prototype and empirically evaluate proposed designs.

In Chapter 8, Dedication of Commercial Off-the-Shelf Hardware and Software, the committee recommends that the USNRC establish what, if any, research is needed with respect to acceptance of COTS in safety applications in nuclear plants.

In Chapter 9, Case-by-Case Licensing Process, the committee recommends that the USNRC catalogue 10 CFR 50.59 evaluations of digital upgrades in some centralized fashion. It is recommended that this cataloguing be studied in a way that lessons learned can be distilled and transmitted to the industry and to all cognizant NRC review staff.

In addressing the technical infrastructure issue, the subject of the present chapter, the committee noted a fundamental problem that affects the nuclear industry as well as the nuclear regulators. This problem is the historical reliance on the professional societies and industry groups to create and update the needed standards and guidance documents, largely through volunteer committees. This approach was effective in the past because the technologies of interest evolved rather slowly and cycle times of one to a few years were acceptable. The generation time for the digital-based technologies is much shorter and the committee-based approach cannot keep up with the industry. This is made worse by the fact that the nuclear industry is not a large, influential customer of the digital I&C industry and it has difficulty in imposing its requirements. As a result, the nuclear industry and its regulators can become technically isolated and the gap could widen with time. A more proactive, efficient method is needed to develop and keep the nuclear-related digital I&C standards up to date. Although the USNRC staff has begun to be more aggressive and participates early in the industry committees and working groups, which is very helpful, by itself this increased participation is not likely to be sufficient. In Chapter 9, the committee recommends the use of chartered task groups to address this need, and that recommendation is reiterated here in view of its importance to assuring adequate technical infrastructure, not only to the regulators but to the industry as a whole.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Conclusion 1. The USNRC should make changes in its staffing, training, and research program to support its regulation of digital I&C technology in nuclear power plants. Specific recommendations are provided below.

Conclusion 2. The issue of adequate technical infrastructure is applicable not only to the USNRC but also to the nuclear industry as a whole. Many of the committee's recommendations for the USNRC have parallel applications to the nuclear industry.

Conclusion 3. The USNRC must anticipate that the regulatory technical infrastructure will continue to be challenged by advancing digital I&C technology. The focus of the near-term licensing effort will be on digital upgrades and certification of the advanced plants. The USNRC will have to continue to expand its technical infrastructure as use of digital technology expands and its sophistication increases.

Conclusion 4. There are problems inherent in the historical process for developing standards and industry guidelines, particularly those applied to the rapidly advancing digital technology. Pending development of alternate approaches, early involvement by the USNRC in developing standards and industry guidelines will foster more timely availability of regulatory guidance and acceptance criteria.

Conclusion 5. A strategic plan is needed for the USNRC research program on digital I&C applications. The current research program is a disjointed collection of studies lacking an underlying strategy and in some specific cases pursuing topics of questionable worth. The staff structure of the USNRC, which separates the staff of the Office of Nuclear Reactor Regulation (NRR) from the staff of the Office of Nuclear Regulatory Research (RES) and mandates that the RES staff respond to NRR "user needs," may be an obstacle to development of a coherent plan that balances near-term regulatory decision making and long-term research into problems on the horizon. Periodic outside review of the USNRC research program could help assure that the right issues are being addressed and could also lead to areas of collaborative research. The committee is aware of and notes favorably the impact of the existing Nuclear Safety Research Review Committee. However, a more formal, outside review would be useful. Perhaps this could be done on an exchange basis with other agencies to reduce resource demands.

Recommendations

Staffing

Recommendation 1. Despite difficulties posed by declining budget and staffing levels in the face of rapidly moving technology and a stagnating nuclear industry, the USNRC must explore ways to improve the efficiency of the review process with existing staff and resources.

Training

Recommendation 2. The USNRC should define a set of minimal and continuing training needs for existing and recruited staff. Particular attention should be paid to software quality assurance expertise. Once defined, the USNRC training program should be subjected to appropriate external review. Certification of USNRC expertise levels is one possibility the USNRC may wish to consider.

Research Plan

Recommendation 3. Consistent with Conclusion 5 above, the USNRC should develop a strategic plan for the research program conducted by the RES and NRR offices. The plan should emphasize balancing short-term regulatory needs and long-term, anticipatory research needs and should incorporate means of leveraging available resources to accomplish both sets of research objectives. It should also reach out more effectively to relevant technical communities (e.g., by the establishment of research simulators for human factors research), to the Electric Power Research Institute, to the Department of Energy, to foreign nuclear organizations, and to other safety-critical industries dealing with digital I&C issues. In making this recommendation, the committee recognizes the Halden Reactor Project provides an example of such cooperative research; but much of the Halden work cannot be published widely and therefore lacks the benefit of rigorous peer scrutiny.

Recommendation 4. Because research in the digital I&C area may require a longer time frame than that of single fiscal years, the USNRC should give consideration to planning and arranging funding on a multiyear basis.

General

Recommendation 5. Consistent with Conclusion 4 above, the USNRC should consider ways to accelerate preparation and updating of needed standards and guidance documents. In particular, the USNRC should consider using chartered task groups (see Recommendation 3 in Chapter 9).

REFERENCES

Jackson, S. 1995. Letter from Shirley Jackson (Chairman, USNRC) to James Taylor (Executive Director for Operations, USNRC), November 30, 1995. Washington, D.C.

Lewis, H. 1992. Digital Instrumentation and Control Systems. Letter to I. Selin, Chairman, USNRC, dated December 11, 1992.

NSRRC (Nuclear Safety Research Review Committee). 1994. Summary of November 29–30, 1993 Meeting of Subcommittee on Advanced Instrumentation and Controls and Human Factors. Letter to E. Beckjord, USNRC, dated January 14, 1994.

USNRC (U.S. Nuclear Regulatory Commission). 1995. Internal audit by USNRC inspector general, December 27, 1995. Washington, D.C.

Utsumi, M. 1996. Mitsubishi Heavy Industries, presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, San Francisco, Calif., January.

11

Overview and Summary

As the study progressed the committee recognized there are two major intertwined themes associated with the use of digital instrumentation and control in nuclear power plants. These are:

1. Dealing with the specific characteristics of digital instrumentation and control (I&C) technology as applied to nuclear power plants.
2. Dealing with a technology that is more advanced than the one widely in use in the existing nuclear power plants. This technology is rapidly advancing at a rate and in directions largely uncontrolled by the nuclear industry but at the same time likely to have a significant impact on the operation and regulation of nuclear power plants.

The technical issues the committee focuses on in this report are primarily related to digital technology itself (Theme 1), while the strategic issues are primarily related to the process of adopting advanced technology (Theme 2). Specifically, the issues largely related to digital technology are systems aspects, software quality assurance, common-mode software failures, quantitative assessment, human factors and human-machine interfaces, and commercial off-the-shelf equipment and systems. The strategic issues, which are not so tightly coupled to the digital technology, are two: case-by-case licensing and technical infrastructure. Although this alignment of issues with themes is not perfect insofar as some of the issues have elements belonging to both themes, nonetheless considering the issues in this way provides a useful framework for the overall discussion.

A major impediment to having this discussion, however, was discovered by the committee in the communication barriers that exist among the key technical communities and individuals involved. The committee itself, most of whose members have been active participants in one or more technical areas associated with digital instrumentation and control, brought a wealth of experience to the consideration of the issues and as a group represented a broad spectrum of the interested parties. Nevertheless, it took an extraordinary effort on the part of the committee to develop a common language and terms and reach a common understanding of the issues themselves, much less agree on ways to build a consensus for addressing these issues. It is clear, both from the committee's interactions with the many individuals who appeared before it and from individual committee members' interactions in their home communities, that this communication problem is widespread.

The basic reason for the communication difficulty is apparent. Work is simultaneously going on at a rapid rate in many areas, each with its own technology, research focus, and agenda. Unfortunately, although many of these areas use common terms, these terms often have different meanings to different groups, resulting in either a lack of communication or very difficult communication. This is particularly troublesome for the nuclear power industry and its regulators, who are not dominant in this technology and must try to synthesize information and experience from a variety of sources and apply it in power plants where safety hazards must be dealt with in a rigorous way, under public scrutiny.

There are a number of ways to address the communication difficulty. Some are already being pursued, some need to be initiated. The committee particularly emphasizes five areas of need:

1. There is a need for better, clearer, crisper statements of the regulatory concern and the appropriate acceptance criteria that are valid at any point in time. As noted in the previous chapters, the committee strongly prefers more focused, succinct statements of regulatory problems, criteria, and standards. This is to be contrasted with the current U.S. Nuclear Regulatory Commission (USNRC) approach which is characterized by relatively complex statements of requirements created by interconnected endorsements and caveats in a family of standards and related documents. The committee understands that the USNRC staff has taken this path as the most efficient in terms of effort and time. But the committee is concerned that the gain in efficiency is

offset by the loss of clarity as to what the regulatory concerns and issues are and the difficulty in clearly defining the related acceptance criteria. On the other hand, it is very important to recognize that criteria for regulation cannot always be quantitative and objective. For today's complex systems, this is clearly not always feasible. Human reliability is a case in point. One must do the best one can with a thoughtful mix of objectivity and expert judgment (subjectivity), given a finite budget.

2. There is a need for the nuclear power industry and the USNRC to be more proactive in the relevant technical communities. Their involvement is needed to be sure that valid issues and constraints, unique to the nuclear power industry, are recognized and addressed. Active involvement also helps the nuclear power community gain access to the broad expertise available in closely related but nonnuclear fields, e.g., software engineering.
3. There is a need for the nuclear power industry and its regulator to strengthen its technical infrastructure in digital systems. It is especially necessary in this area to work cooperatively and creatively to husband and multiply the available resources, by working together and carefully selecting the topics to be pursued. The committee recognizes the need for the regulator to be independent but sees maintaining this independence as feasible. The committee also sees some progress in this regard, particularly in early involvement by the regulators in reviewing and assessing industry research programs and guidelines development efforts and in new training programs for the USNRC staff. The committee commends those efforts and urges their expansion to make best use of the limited resources available.
4. There is a need to formally address the communication problem in a systematic way. This would include increased attention in documents to the clear definition of terms and context. The committee also suggests increased use of early, informal communication between the USNRC staff and the industry in areas where there is uncertainty or lack of clear regulatory guidance.
5. There is a need to tune up the regulatory mechanisms that are employed when an advanced technology, like digital I&C, has temporarily outpaced the regulations. Such a mechanism is 10 CFR 50.59, which the committee believes is fundamentally sound and should continue to be used. But, as discussed particularly in Chapter 9 (Case-by-Case Licensing Process), there are a number of changes that could be made to the regulatory process that would make this process much more efficient and assure that the intent and basis of the decisions made are fully communicated.

Turning to high-level issues more specifically related to digital technology, the committee emphasizes the following:

1. Deterministic assessment methodologies, including design basis accident analysis, hazard analysis, and other formal analysis procedures, are applicable to digital systems, as long as they are applied with care.
2. There is controversy within the software community as to whether an accurate failure probability can be assessed for software or even whether software fails randomly. However, the committee agreed that a software failure probability can be used for the purposes of performing probabilistic risk assessment (PRA) in order to determine the relative influence of digital system failure on the overall system. Explicitly including software failures in a PRA for a nuclear power plant is preferable to the alternative of ignoring software failures.
3. Digital I&C systems (and digital systems in general) should not be addressed only in terms of hardware or software. Hardware and software must be treated together as a system; focusing solely on one or the other should be done with great caution. There are two examples from this report: First, the treatment of "common-mode software errors" leads far beyond the boundaries of the software itself; and the successful resolution of this problem emphasizes treatment of the systems as a whole. A second example is the treatment of complexity. It is important to assure that system complexity is addressed. For example, digital system complexity issues are not resolved by simplifying the software dramatically at the expense of introducing more complex (and potentially less testable) hardware.
4. Most practical digital I&C systems cannot be exhaustively tested and therefore cannot be shown to be free from any and all errors. However, the committee is convinced that adequate approaches exist and can be applied within practical resource restraints to support the use of digital systems in safety-critical applications in nuclear power plants.

In summary, the committee notes that digital instrumentation and control is state-of-the-art technology and is widely used both inside and outside the nuclear industry. Digital I&C systems offer powerful capabilities that can, however, affect nuclear power plant safety; therefore, digital systems should be treated carefully, particularly in safety-critical applications. It appears the USNRC and the nuclear power industry are moving forward with procedures, processes, and technical infrastructure needed to assure continued safe operation of the plants. The committee has suggested several improvements. Given this situation, the committee considers the use of digital I&C systems in new nuclear power plants and in modifications and upgrades of existing plants to be appropriate and desirable. For existing plants, this is particularly true where digital I&C systems replace older systems and equipment for which vendor support is no longer readily available.

APPENDICES

APPENDIX A

Biographical Sketches of Committee Members

DOUGLAS M. CHAPIN (chair) is principal officer, MPR Associates, Inc., an Alexandria, Virginia, based engineering firm. He has practiced electrical, chemical, and nuclear engineering since 1962. This has included analysis of plant performance in steady-state, transient, and accident conditions. Particular areas of experience include electrical and fluid system design; instrumentation and control systems; nuclear fuel and reactor structural design; nuclear safety system design, analysis, and testing; fire protection; and quality assurance. He has worked closely with the Electric Power Research Institute on projects such as the Advanced Light Water Reactor Program and the Utility Review Committee on Advanced Reactor Designs. He has also managed and directed numerous activities at MPR on U.S. and foreign digital instrumentation and control systems. His most recent paper, presented at the Third International Conference on Nuclear Engineering, is titled "Advanced Instrumentation and Control and Human-Machine Interface Systems for Nuclear Power Plants." He received a BSEE from Duke University, an MSE from George Washington University, and a Ph.D. in nuclear studies in chemical engineering from Princeton University.

JOANNE BECHTA DUGAN is associate professor of electrical engineering at the University of Virginia. Previously she was associate professor of computer science at Duke University and visiting scientist at the Research Triangle Institute. She has performed and directed research on the development and application of techniques for the analysis of computer systems which are designed to tolerate hardware and software faults. Her research interests thus include hardware and software reliability engineering, fault tolerant computing, and mathematical modeling using dynamic fault trees, Markov models, Petri nets, and simulation. Dr. Bechta Dugan is an associate editor of the *IEEE Transactions and Reliability*, is a senior member of the IEEE, and is a member of Eta Kappa Nu and Phi Beta Kappa. She received a B.A. from La Salle University, and an M.S. and a Ph.D. in electrical engineering from Duke University.

DONALD A. BRAND is a lecturer with the Department of Civil Engineering, University of California, Berkeley, California. In 1995, he retired from the Pacific Gas and Electric (PG&E) Company as senior vice president and general manager, Engineering and Construction Business Unit. During his 33 years with PG&E, he carried out numerous managerial and engineering responsibilities with respect to the design, construction, and operation of fossil, geothermal, nuclear, and hydroelectric generating facilities, together with electrical transmission, distribution, and power control facilities. Industry activities have included membership on the Electric Power Research Institute's Research Advisory Committee and the Association of Edison Illuminating Company's Power Generation Committee. Currently, he is a member of the National Academy of Engineering, a registered nuclear engineer in the state of California, and a vice president of the U.S. National Committee of the International Conference on Large High Voltage Electric Systems. He received a B.S. in mechanical engineering and an M.S. in mechanical (nuclear) engineering from Stanford University. He also graduated from the Advanced Management Program of the Harvard University School of Business.

JAMES R. CURTISS is a partner in the law firm of Winston and Strawn in Washington, D.C., where he specializes in nuclear regulatory law. Prior to his present position, he served as commissioner of the U.S. Nuclear Regulatory Commission (1988–1993). He previously served as counsel to the Subcommittee on Nuclear Regulation of the Senate Committee on Environment and Public Works. Prior to that, he was a lawyer in the Office of the Executive Legal Director of the U.S. Nuclear Regulatory Commission. He also served on the staff of USNRC Commissioner Richard T. Kennedy. He is a member of the bar of the District of Columbia Court of Appeals, the state of Nebraska, and the U.S. Supreme Court. He is also a member of the American Nuclear Society, the Society for Risk Analysis, and the District of Columbia Bar Association. He is a director of the Baltimore Gas and Electric Company and Cameco Corporation, and is a member of the Institute of Nuclear Power Operation's Advisory Council. He has also served as a member of a recent National Research Council committee panel charged with advising the Department of Energy on its environmental remediation program. He received a B.A. and a J.D. from the University of Nebraska.

D. LARRY DAMON is manager of engineering technology, Bechtel Research and Development, San Francisco. Previously, he held a variety of technical positions at Bechtel, including project manager in the development of the Simplified Boiling Water Reactor and chief engineer for Control Systems. Prior to joining Bechtel, he was a project engineer with Tracerlab Incorporated, where he was responsible for the design, development, and implementation of land-based nuclear reactor monitoring systems. He has 32 years of engineering and management experience in the nuclear power field with special technical emphasis on multidiscipline design integration, computer-based controls and simulations, nuclear instrumentation, systems engineering, and human factors. He has extensive field experience in the areas of design change control, design implementation and expediting, operational testing, and startup. He received a bachelor's degree in electrical engineering from the University of Nevada.

MICHAEL DEWALT is national resource specialist for software for the Federal Aviation Administration in Seattle. He is responsible for providing technical guidance concerning policy, training, and research and development in the area of embedded real-time reactive software that is used aboard aircraft and their associated ground-based interfaces. He is the technical focal point for industry and the FAA for the evaluation of new technology and the interpretation of existing policy as applied to aircraft systems. Previously, he has worked as a software life-cycle consultant for Telos Consulting Services, a software control system engineer for Pacific Technologies Incorporated, an avionics certification engineer for the FAA, the software focal point for the autopilot on the Boeing 757/767 digital aircraft for Boeing, and a digital and analog avionics engineer for Honeywell Flight Systems. He has made a number of presentations at international conferences on the subject of assuring safety-critical software-based systems. He is a member of the Institute of Electrical and Electronic Engineers' working groups drafting new standards for safety-critical software and revising IEEE document 1012, Standards for Verification and Validation. He is also a member of the Association of Computing Machinery and a past member of its working group charged with defining qualifications for software professionals. He received a B.S. in electrical engineering from the University of Washington and an M.S. in software engineering from Seattle University.

JOHN D. GANNON is professor and chair of the Department of Computer Science at the University of Maryland, where he has been a faculty member since 1975. He conducts research on automated applications of formal methods to software development activities, e.g., proving that requirements enforce safety properties and deriving test oracles from formal specifications. He has also worked for the National Science Foundation as program director for software engineering. During the past several years, he has served on a National Research Council committee assessing the adequacy of independent verification and validation for NASA's space shuttle avionics software. He has also helped the Argonne National Laboratory evaluate software development processes for trusted systems and the USAF Science Advisory Board examine procedures for software acceptance testing. He is a member of the editorial boards of *IEEE Transactions on Software Engineering* and *ACM Computing Surveys*. He received a Ph.D. in computer science from the University of Toronto.

ROBERT L. GOBLE is research professor of environment, technology, and society and adjunct professor of physics at Clark University. Previously he was assistant professor, Department of Physics, Montana State University; research associate, Department of Physics, University of Utah; research associate, Department of Physics, University of Minnesota; research assistant/instructor, Department of Physics, Yale University; and NSF Cooperative Fellow, Department of Physics, University of Wisconsin. His recent research activities include risk assessment methodology, environmental and occupational impacts on health, sustainable development and climatic change, nuclear safety and economics, and ethical issues in hazard management. He has produced numerous publications and provided testimony pertaining to nuclear power plant risk assessment. His most recent work is entitled "What Nuclear Emergency Planning Can and Cannot Accomplish," published in *Preparing for Nuclear Power Plant Accidents: Selected Papers*. He received a Ph.D. in physics from the University of Wisconsin.

DAVID J. HILL is associate director for Reactor Plant Safety and Operations, Reactor Analysis Division, Argonne National Laboratory, Argonne, Illinois. He also directed system safety assessments for reactor and nonreactor facilities and reliability analysis using fault tree and event tree techniques, including human reliability assessments. Recently, he was awarded the University of Chicago's highest award, the University of Chicago Distinguished Performance Award, for his work in guiding the Level One Probabilistic Risk Assessment of the Experimental Breeder II Reactor. His program management experience includes a variety of positions in the United Kingdom and United States. He received a Ph.D. in mathematical physics from the Imperial College of London.

PETER E. KATZ is plant manager, Calvert Cliffs Nuclear Power Plant, Lusby, Maryland. Previously, he held various positions at Baltimore Gas and Electric Company, including manager of Nuclear Engineering, superintendent of technical support, and general supervisor of Design Engineering at Calvert Cliffs. He has also served as general supervisor of maintenance and modifications in Fossil Engineering Services and principal engineer in the Instrumentation and Control Unit. His responsibilities have included plant design support, design engineering, nuclear regulatory matters, technical services engineering, and instrumentation and control systems. He is chairman of EPRI's Nuclear Power Division I&C Obsolescence Cost Control Committee, a member of the Nuclear Power Division Business Unit Council, and a previous member of their Nuclear Safety Analysis Center. He received a B.S. in electric power engineering at Rensselaer Polytechnic Institute and an M.S. in environmental engineering from Johns Hopkins University.

NANCY G. LEVESON is Boeing Professor of Computer Sciences and Electrical Engineering, University of Washington, and adjunct professor, University of British Columbia. Her research interests include software engineering, systems and software safety and reliability, and formal modeling and mathematical analysis of embedded systems. She consults worldwide for industry and government on the introduction of computers to control defense, aerospace, transportation, medical, and nuclear systems. She is the editor-inchief of *IEEE Transactions on Software Engineering*, a member of the board of directors of the Computing Research Association, and a member of the Association for Computing Machinery Committee on Computers and Public Policy. She is a fellow of the ACM and received the 1995 AIAA Information Systems Award for contributions in space and aeronautics technology and research. She was the U.S. Representative to the Advisory Group on Computers in Nuclear Power Plants of the United Nations International Atomic Energy Agency. She is a member of the Commission on Engineering and Technical Systems of the National Research Council. She recently chaired a study of the space shuttle flight software processes for the National Research Council. She received a B.A. in mathematics, an M.S. in management (operations research), and a Ph.D. in computer science from the University of California, Los Angeles.

CHRISTINE M. MITCHELL is professor of industrial and systems engineering and adjunct professor of computer science, Georgia Institute of Technology. Her research interests include operator aids, intelligent training systems, and applications of artificial intelligence. She has published over 100 papers in technical journals, books, and conference proceedings. Her most recent work is titled "Human-Machine System Models: A Prerequisite to the Design of Human-Computer Interaction in Complex Dynamic Systems." She has also received several grants from NASA for research in intelligent command and control systems and human-centered design of human computer interactions. She is an associate editor of the *IEEE Transactions on Systems, Man, and Cybernetics* and of *Automatica* and a technical reviewer for NSF, NASA, and numerous technical journals. She earned a Ph.D. in industrial and systems engineering from Ohio State University.

CARMELO RODRIGUEZ is manager of Control and Robotics Engineering at General Atomics in San Diego. Previously, he was project engineer and group leader, Gulf Research and Development Co. His professional specialties include automatic control, materials handling, robotics, instrumentation, and electrical engineering. He has led the design and development of nuclear fuel handling and accountability systems, digital control and protection systems for nuclear and petrochemical plants, distributed digital radiation monitoring systems for light water reactors, and nuclear compact simulators. He has served in field engineering positions as part of startup and on operations and maintenance task forces in nuclear plants and petroleum refineries. He has been a U.S. delegate to International Atomic Energy Agency meetings on nuclear instrumentation and has published numerous papers on process control, operations, and maintenance. He is a member of the IEEE and received an M.S. and a Ph.D. in electrical engineering from the University of Pittsburgh.

JAMES D. WHITE is section head for Controls and Systems Integration and coordinator of Advanced Instrumentation, Oak Ridge National Laboratory. Previously he held various positions at the laboratory, including technical director of Liquid Metal Reactor Programs and Light Water Reactor Programs and manager of the Advanced Controls Program. His past work has involved R&D in man-machine interfaces, networking of computers, adaptive control techniques, modern and classical control theory, signal validation, and balance of plant control prototypes. He organized and co-chaired the NSF Panel on Assessment of Instrumentation and Control Technologies for European Nuclear Power Plants and served on the NSF Panel on Assessment of Japanese Nuclear Power. He received his B.S. and M.S. in nuclear engineering from the University of Tennessee.

APPENDIX B

Committee Meetings (Phases 1 and 2)

PHASE 1

First Meeting

January 31–February 2, 1995
National Research Council
Washington, D.C.

Presentations:

Study Background and Expectations from Sponsor
Leo Beltracchi, USNRC Office of Nuclear Regulatory Research (USNRC/RES), Staff Member, Controls, Instrumentation, and Human Factors Branch

Advisory Committee on Reactor Safeguards (ACRS): Individual Member Perspectives
Thomas Kress, Chairman; William Shack, Member; Douglas Coe, Staff; Chad Litte, Intern

Nuclear Safety Research Review Committee (NSRRC) Perspectives
David Morrison, former Chairman (and designated as incoming Director of USNRC/RES); Robert Uhrig, Member

Office of Nuclear Regulatory Research (RES) Perspectives
Eric Beckjord, USNRC, Director, Office of Nuclear Regulatory Research (retired April 1995)

Regulatory Process Overview
Jared Wermiel, USNRC Office of Nuclear Reactor Regulation (USNRC/NRR), Chief, Instrumentation and Controls Branch

Nuclear Power Plant I&C System Design
Clifford Doutt, USNRC/NRR, Senior Electrical Engineer; Matthew Chiramal, USNRC/NRR, Section Chief, Advanced Reactors

Regulating Digital Upgrades
Jerry Mauck, USNRC/NRR, Section Chief, Operating Reactors

Instrumentation and Control Current Safety Issues
Jerry Mauck, USNRC/NRR, Section Chief, Operating Reactors

The State-of-the-Art in Digital I&C Systems in Nuclear Power Plant Applications
Jerry Mauck, USNRC/NRR, Section Chief, Operating Reactors; Matthew Chiramal, USNRC/NRR, Section Chief, Advanced Reactors

Second Meeting

March 2, 1995
Arnold and Mabel Beckman Center
Irvine, California

Committee discussions and deliberations.

Third Meeting

April 12–13, 1995
Chattanooga, Tennessee

Site Visits:

Committee visits to the Nuclear Regulatory Commission's Technical Training Center in Chattanooga, to view both an analog and a digital-based simulator; the Sequoyah Nuclear Power Plant in Soddy-Daisy, Tennessee, which was recently upgraded with the Eagle 21 (digital) reactor protection system; and Georgia Power's Hammond Power Plant, a fossil-fueled power plant in Rome, Georgia, which includes digital controls.

Fourth Meeting

August 9–11, 1995
National Research Council
Washington, D.C.

Committee discussions and deliberations.

PHASE 2

Fifth Meeting

October 16–18, 1995
National Research Council
Washington, D.C.

Presentations:

Discussion of Systems Issues of Digital Instrumentation and Control Technology
James Keiper, Industry Consultant, Nuclear Systems, Foxboro Company

Current USNRC Activities Related to the Phase 1 Report:

Introductory Remarks
Franklin Coffman, USNRC/RES, Chief, Controls, Instrumentation, and Human Factors Branch

Strategic Issues
Jared Wermiel, USNRC/NRR, Chief, Instrumentation and Controls Branch

Technical Issues
Matthew Chiramal, USNRC/NRR, Instrumentation and Controls Branch, Section Chief, Advanced Reactors

Human-Machine Interface Issue
Richard Eckenrode, USNRC/NRR, Staff Member, Human Factors Assessment Branch

Strategic and Technical Issues
Leo Beltracchi, USNRC/RES, Staff Member, Controls, Instrumentation, and Human Factors Branch

Human-Machine Interface Issue
Jay Persinski, USNRC/RES, Staff Member, Controls, Instrumentation, and Human Factors Branch

Adequacy of Technical Infrastructure
Steve Arndt, USNRC Technical Training Center

Summary Remarks
Franklin Coffman, USNRC/RES, Chief, Controls, Instrumentation, and Human Factors Branch

Sixth Meeting/Workshop

December 13–15, 1995
National Research Council
Washington, D.C.

Presentations:

Discussions on Digital Instrumentation and Control and Each of the Eight Issues with Representatives from the U.S. Nuclear Industry
Bruce Geddes, Baltimore Gas and Electric, Calvert Cliffs Nuclear Power Plant; Charles Waite, Public Service Electric and Gas Company, Salem Nuclear Power Plant; and Gerry Van Noordenen, Northeast Utilities, Millstone Nuclear Power Plant

Discussion of Systems Aspects of Digital Instrumentation and Control
Al Sudduth, Duke Power

Discussion of Common-Mode Software Failure Potential
Grady Lee, Consultant; Mike Brown, Naval Surface Warfare Center; John Knight, University of Virginia

Discussion of Software Quality Assurance
Paul Joannou, Ontario Hydro

Seventh Meeting

January 16–18, 1996
Bechtel Research and Development
San Francisco, California

Presentations:

The Federal Aviation Administration (FAA) Software Quality Assurance Process
Mike DeWalt, FAA/Committee Member

Discussions on Digital Instrumentation and Control and Each of the Eight Issues
Masafumi Utsumi, Senior Engineer, Mitsubishi Heavy Industries, Ltd., Japan

Digital I&C Upgrade Experience at the Pacific Gas and Electric Company's Diablo Canyon Nuclear Plant
Bob Webb, Klemme Hermann, and John Hefler, Pacific Gas and Electric Company

Discussions about the Electric Power Research Institute (EPRI) Digital I&C Licensing Guideline
Dan Wilkinson and Ray Torok, EPRI

Current USNRC Human-Machine Interface (HMI) Guidance and Results from the Halden Reactor Project
Leo Beltracchi and Dick Eckenrode, USNRC

EPRI Research on the Effects of Digital Instrumentation and Control on HMI
Lewis Hanes, EPRI

NASA HMI Research
Mike Shafto, NASA Ames Research Center

Reliability Assessment Methods Applied to the Boeing 777 Avionics Program
Frank McCormick, Consultant/Former Boeing Engineer

Use of PRA and Other Reliability Assessment Methods Applied to Digital Instrumentation and Control
George Apostolakis, MIT

Eighth Meeting

February 28–March 1, 1996
Arnold and Mabel Beckman Center
Irvine, California

Presentations:

Dedication of Commercial Off-the-Shelf Hardware and Software and the Electric Power Research Institute Working Group
Ray Torok, EPRI

Discussion of Systems Issues of Digital Instrumentation and Control Technology
Barry Simon, General Electric

Formal Methods, the Certification of Safety-Critical Systems, and Differences Between Safety and Reliability
John Rushby, SRI International/Computer Science Laboratory

Ninth Meeting

April 16–18, 1996
National Research Council
Washington, D.C.

Presentations:

Reliability Assessment Methods Applied to Other Safety-Critical Industries
Joseph Profetta, Union Switch and Signal; Lynn Elliott, Guidant Cardiac Pacemakers Incorporated

Discussion of Systems Issues of Digital Instrumentation and Control Technology, Eagle 21, and Sizewell-B
Carl Vitalbo and William Ghrist, Westinghouse

USNRC Position on Common-Mode Software Failure Potential
Jared Wermiel, USNRC/NRR, Chief, Instrumentation and Controls Branch; Martin Malsch, Deputy General Counsel, USNRC

Current State of Design Guidance for Human Factors in Digital Systems
David Woods, Ohio State University

Tenth Meeting

May 20–22, 1996
National Research Council
Washington, D.C.

Committee discussions and deliberations.

Eleventh Meeting

June 24–26, 1996
National Research Council
Washington, D.C.

Committee discussions and deliberations.

Twelfth Meeting

October 15–17, 1996
National Research Council
Washington, D.C.

Committee discussions and deliberations.

APPENDIX C

U.S. Nuclear Regulatory Commission Licensing of Digital Instrumentation and Control Technology

In the regulation of digital instrumentation and control (I&C) technology, the U.S. Nuclear Regulatory Commission (USNRC) has considered both retrofits to existing, operating plants and implementation of digital I&C technology in new plants of advanced design.

OPERATING PLANTS

The USNRC has approved a number of retrofits of digital I&C systems in existing nuclear power plants. These retrofits have ranged from small-scale replacements of individual components to full reactor protection system upgrades.

The first replacement of a full reactor protection system was at the Connecticut Yankee's Haddam Neck station in 1991. The Haddam Neck upgrade was followed by retrofits at the Sequoyah, Zion, Diablo Canyon, and D.C. Cook nuclear power plants.

As expressed in their safety evaluations of the above upgrades, the USNRC concluded that the application of programmable digital devices in redundant nuclear safety systems introduces the possibility of common-mode software failure, which could jeopardize the redundancy and independence features of the plant protection system (as discussed in General Design Criterion 22, Regulatory Guide 1.75, and IEEE-STD-279).

The concern about common-mode software failure led the USNRC to conclude that all future digital upgrades would involve an "unreviewed safety question" (USQ) as defined by 10 CFR 50.59. Determination that an upgrade involves a USQ mandates formal plant license amendments under 10 CFR 50.90. These license amendments typically entail a prolonged, customized review process and public hearings for each upgrade. The additional time and expense inherent in the customized review process has created substantial disincentives for the utilities to pursue digital I&C upgrades.

To be even clearer on the issue and to provide all licensees a better understanding of their position, the USNRC distributed a draft generic letter outlining why such upgrades presented a USQ and thus could not proceed without prior approval. However, the nuclear industry does not consider most digital I&C upgrades to involve a USQ. In an attempt to resolve the disagreement, the nuclear industry developed guidelines (EPRI, 1993). These guidelines were developed in coordination with the USNRC staff. While the USNRC has endorsed the nuclear industry guidelines, it has offered clarifications that appear to leave the situation unresolved (USNRC, 1995).

NEW PLANTS

The USNRC is reviewing a number of advanced nuclear power plant designs. These designs include the General Electric (GE) Advanced Boiling Water Reactor (General Electric, 1994), the GE Simplified Boiling Water Reactor, the Westinghouse AP600, and the Asea Brown Boveri (ABB) Combustion Engineering System 80+ (Combustion Engineering, 1993). The I&C systems in these advanced plant designs are all-digital systems intended to utilize and exploit the new technology.

The light-water reactor designs follow the guidelines of the nuclear industry's Advanced Light Water Reactor Utility Requirements Document (EPRI, 1992). The USNRC has evaluated these guidelines (USNRC, 1994) but did not fully resolve many of the issues involved in the application of digital I&C technology.

The USNRC has issued a final design approval on two advanced plant designs (Combustion Engineering, 1993; General Electric, 1994) under a new regulatory review process. Certification of these two plant designs is proceeding. In advanced plants, the design review by the USNRC covers only the design process, since actual plant hardware (and software in the case of digital I&C systems) is not yet available for review. Therefore, the USNRC may have continuing difficulty in the final certification of advanced designs unless the issues surrounding certification of digital I&C technology are resolved.

STANDARDS DEVELOPMENT

The USNRC has worked with the nuclear industry and professional societies in continuing to develop standards for digital I&C applications in nuclear power plants. Several USNRC guidelines are in place (USNRC, 1981, 1991) and other industry standards have been developed (such as ANSI/IEEE-ANS 7.4.3.2, ANSI/IEEE-Std-1012-1986, ASME NQA 2A-1990, Regulatory Guide 1.152). The USNRC has continued development of additional guidance such as draft "Branch Technical Positions" and other documents (see, e.g., USNRC, 1994, 1995; Wermiel, 1995). In addition, the USNRC has conducted a series of meetings with its advisory groups (see, e.g., ACRS, 1992a, 1992b; NSRRC, 1992), solicited research papers (see, e.g., NRC, 1988), and organized workshops (USNRC, 1993a). The USNRC's Office of Nuclear Regulatory Research also supports research into several areas relevant to the present problem of evaluating and regulating digital I&C technology. However, these efforts have not yet been able to provide the necessary answers.

RECENT DEVELOPMENTS

Recent USNRC positions (Mauck, 1995) indicate the USNRC's willingness to clarify their requirements and define acceptable standards. The USNRC will still require demonstration of defense-in-depth as described in NUREG-0493, but it will also tolerate disablement of a safety function by a common-mode failure if a diverse set of equipment not subject to the same failure can perform the same safety function. Moreover, in demonstrating such diversity, the USNRC will allow the use of digital or analog based nonsafety systems and operator actions. In recent licensing positions (USNRC, 1993b), the USNRC further indicated its acceptance of adequate software reliability based on prior audits of a supplier's verification and validation program. Still, and in spite of substantial effort by the USNRC and the industry, a sufficiently definitive set of generic guidelines does not exist and the docketed case-by-case method of prior approval remains necessary. For this reason, the USNRC's efforts are continuing (Wermiel, 1995) and, in cooperation with the Advisory Committee on Reactor Safeguards, are responsible for the study being performed under the auspices of the National Research Council (ACRS, 1994).

REFERENCES

ACRS (Advisory Committee on Reactor Safeguards to the U.S. Nuclear Regulatory Commission). 1992a. Digital Instrumentation and Control System Reliability. Letter to I. Selin, Chairman, USNRC, September 16, 1992.

ACRS. 1992b. Minutes of ACRS Subcommittee Meeting on Computers in Nuclear Power Plant Operations: Special International Meeting, September 22, 1992.

ACRS. 1994. Proposed National Academy of Sciences/National Research Council Study and Workshop on Digital Instrumentation and Control Systems. Letter to I. Selin, Chairman, USNRC, July 14, 1994.

Combustion Engineering. 1993. The Certified Design Material (ITAAC) for the System 80+ Standard Plant from ABB Combustion Engineering, Inc., Section 2.5, Instrumentation and Control. Windsor, Conn.: Combustion Engineering.

EPRI (Electric Power Research Institute). 1992. Advanced Light Water Reactor Utility Requirements Document. EPRI NP-6780-L, Vol. 2 (ALWR Evolutionary Plant) and Vol. 3 (ALWR Passive Plant), Ch. 10: Man-Machine Interface Systems. Palo Alto, Calif.: EPRI.

EPRI. 1993. Guideline on Licensing Digital Upgrades. EPRI TR-102348. Palo Alto, Calif.: EPRI.

General Electric. 1994. Advanced Boiling Water Reactor Final Safety Evaluation Review. Ch. 18: Human Factors Engineering. San Jose, Calif.: General Electric.

Mauck, J. 1995. Regulating Digital Upgrades. Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Washington, D.C., January 31.

NRC (National Research Council). 1988. Human Factors Research and Nuclear Safety. Committee on Human Factors, National Research Council. Washington, D.C.: National Academy Press.

NSRRC (Nuclear Safety Research Review Committee). 1992. Summary of April 29, 1992, Meeting. Letter to E. Beckjord, USNRC, dated November 16, 1992.

USNRC (U.S. Nuclear Regulatory Commission). 1981. USNRC Standard Review Plan (SRP), NUREG-0800, section 7.1, Instrumentation and Controls. Other sections applicable to instrumentation and control technology include: 3.10, Seismic and Dynamic Qualification of Mechanical and Electrical Equipment; 3.11, Environmental Qualification of Mechanical and Electrical Equipment; 4.4, Thermal and Hydraulic Design; 7.2, Reactor Trip System; 7.3, Engineered Safety Features Systems; 7.4, Safe Shutdown Systems; 7.5, Information Systems Important to Safety; 7.6, Interlock Systems Important to Safety; 7.7, Control Systems; 8.1, Electric Power; 8.2, Offsite Power System; 8.3.1, A-C Power Systems (Onsite); 8.3.2, D-C Power Systems (Onsite); 15.0, Review of Anticipated Operational Occurrences and Postulated Accidents; 15.1.5, Steam System Piping Failures Inside and Outside of Containment. Washington, D.C.: USNRC.

USNRC. 1991. Digital Computer Systems for Advanced Light Water Reactors. USNRC SECY-91-292. Washington, D.C.: USNRC.

USNRC. 1993a. Proceedings of the Digital Systems Reliability and Nuclear Safety Workshop, September 13-14, 1993, Rockville, Md. NUREG/CP-0136, NIST SP 500-216. Washington, D.C.: U.S. Government Printing Office.

USNRC. 1993b. Safety Evaluation Report by the Office of Nuclear Reactor Regulation Related to Amendment No. 84 to Facility Operating License No. DPR-80 and Amendment No. 83 to Facility Operating License No. DPR-82: Eagle 21 Reactor Protection System Modification with Bypass Manifold Elimination: Diablo Canyon Power Plant. Dockets Nos. 50-275 and 50-323, October 7, 1993. Washington, D.C.: USNRC.

USNRC. 1994. NRC Review of Electric Power Research Institute Advanced Light Water Reactor Utility Requirements Document. NUREG-1242, Vol. 3, Parts 1–2. Washington, D.C.: USNRC.

USNRC. 1995. Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59. NRC Generic Letter 95-02. Washington, D.C.: USNRC.

Wermiel, J. 1995. Update of Instrumentation and Control Systems Section of the Standard Review Plan, NUREG-0800. Presentation to the Advisory Committee on Reactor Safeguards to the U.S. Nuclear Regulatory Commission, Rockville, Md. April 7.

APPENDIX D

Development of the Final List of Eight Issues

At its first meeting, the committee identified and considered a number of issues and facets of issues, as shown in this appendix. These initial deliberations, as well as those of later committee meetings, were analyzed and organized, and they eventually led to the final list of six technical and two strategic issues. This appendix provides an insight into some of these deliberations by listing some of the earlier, more specific, issues and topics tied to each of the final list of eight.

SYSTEMS ASPECTS OF DIGITAL INSTRUMENTATION AND CONTROL TECHNOLOGY

How can potential safety augmentation at the system level by the use of computers (e.g., diagnosis and accident management) be balanced and evaluated against potential safety decreases (e.g., owing to overreliance or to poor design/implementation that does not achieve assumed benefits or makes things worse)?

Performance during transients, anticipated transient without scram (ATWS) issues, fail-safe design (e.g., can failures be detected as easily as with analog devices?). Does the use of computers make any difference in these areas?

Are there new environmental concerns (e.g., electromagnetic interference, climate control)?

What behaviors or features are of concern and how do we provide confidence (assessment) for them (e.g., unintended function, performance issues, capacity and overload, fail-safe design, networking)?

Communications system distractions.

System capacity.

Response time of the system.

Network reliability, especially in advanced plants.

Recognition/detection of failure modes.

Architecture performance during transients.

Integration issues with analog components.

SOFTWARE QUALITY ASSURANCE

How can confidence be obtained in the safety and/or reliability of software? How should software be assessed?

What methods are appropriate and effective (e.g., verification and validation techniques, formal methods, quantification, hazard analysis, failure mode analysis and design)?

Do some software design techniques present special problems in assessment (e.g., artificial intelligence techniques)?

How can it be assured that changes and fixes do not degrade reliability and safety? What changes should require U.S. Nuclear Regulatory Commission (USNRC) approval and which should not? What changes should be instituted for change control? (E.g., should patching be allowed?) How can it be assured that required changes are made?

Confidence level (quality, verification and validation, formal methods, lack of meaningful standards).

Certification basis (process vs. product).

Fear of unintended function(s).

Configuration control (maintenance/upgrading).

Security considerations.

COMMON-MODE SOFTWARE FAILURE POTENTIAL

Are changes needed in the procedures for evaluating common-mode failures?

Reliability vs. safety: Do the enhanced capabilities of software allow new means of protection against computer failures or failure modes?

Quality vs. diversity: How much relative attention should be paid to each?

Diversity achievement.

Progressive approach to failure (defense-in-depth).

SAFETY AND RELIABILITY ASSESSMENT METHODS

Are there any implications for design basis accidents and the procedures for certifying against them?

What are the implications of using computers with respect to probabilistic risk assessment (PRA) procedures and use?

Are we taking solutions for old technology and inappropriately applying them to new technology (e.g., emphasis on diversity and redundancy, bottom-up component reliability approaches vs. risk-based or hazard analysis approaches)? Are there new approaches that may be more appropriate?

Assessment technology.

Added complexity of digital technology compared to analog.

Definition of safety margin with digital technology.

Loss of margin of safety by consolidation of data.

PRA or mathematical assessment method validity with digital technology.

HUMAN FACTORS AND HUMAN-MACHINE INTERFACES

Should restrictions be imposed on the safety or safety-related functions that can be allocated to computers as opposed to operators or analog devices?

Other operator aids such as alarm analysis, value sequencing, and decision analysis.

Task allocation (computer vs. human).

Level of automation.

Human interface (role, display, information, nuances).

Use of "intelligence" aids (e.g., neural nets, artificial intelligence).

Operations and maintenance impacts (pluses and minuses).

DEDICATION OF COMMERCIAL OFF-THE-SHELF HARDWARE AND SOFTWARE

Are special procedures required for software tools (e.g., compilers, code generators)?

What assessment procedures are appropriate for COTS software? How should dedication procedures differ from those used to certify (handle) specially constructed software?

IEEE-STD-279 compliance.

Use of standard software tools/compilers.

CASE-BY-CASE LICENSING PROCESS

Types of software complexity: Should the assessment basis and procedures differ?

Are there fundamental differences in functionality between analog and digital devices, e.g., between their failure modes, and do they affect certification or licensing?

Use of computers in safety compared to nonsafety systems.

Does the use of computers change the basis for certification procedures at the system level?

What should be the limits of the USNRC regulatory activities?

How does the USNRC determine whether safety value has been added or reduced?

Should the certification basis for computers and software be different from that for the analog devices they replace?

How can the USNRC determine whether safety or reliability has been degraded when we retrofit computers into existing designs?

How should version control be managed? Is this a USNRC concern?

Safety/control systems separation in digital as opposed to analog systems.

Lack of understanding of design basis.

Digital value added (e.g., accident diagnosis and management).

Regulatory constraints.

Short half-life of the technology.

ADEQUACY OF TECHNICAL INFRASTRUCTURE

How should the USNRC deal with the rapid changes in technology?

Lack of strategic plan for the USNRC research program.

Other industry experience as part of the USNRC technical basis.

APPENDIX E

Excerpts from Licensing Regulations

SELECTED CRITERIA FROM TITLE 10 CFR PART 50, APPENDIX A

[Reproduced below are selected criteria from the General Design Criteria (Title 10 CFR Part 50, Appendix A) of particular significance in nuclear power plant applications of digital instrumentation and control (I&C) systems.]

Criterion 1. Quality Standards and Records

Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

Criterion 10. Reactor Design

The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

Criterion 13. Instrumentation and Control

Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

Criterion 19. Control Room

A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident.

Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Criterion 20. Protection System Functions

The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

Criterion 21. Protection System Reliability and Testability

The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Criterion 22. Protection System Independence

The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Criterion 23. Protection System Failure Modes

The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

Criterion 24. Separation of Protection and Control Systems

The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Criterion 25. Protection System Requirements for Reactivity Control Malfunctions

The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control system, such as accidental withdrawal (not ejection or dropout) of control rods.

Criterion 29. Protection Against Anticipated Operational Occurrences

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety function in the event of anticipated operational occurrences.

10 CFR 50.59 CHANGES, TESTS, AND EXPERIMENTS

[Reproduced below are the requirements for changes, tests, and experiments (10 CFR 50.59) in nuclear power plants. These requirements hold particular significance for applications of digital I&C systems.]

(a)(1) The holder of a license authorizing operation of a production or utilization facility may (i) make changes in the facility as described in the safety analysis report, (ii) make changes in the procedures as described in the safety analysis report, and (iii) conduct tests or experiments not described in the safety analysis report, without prior Commission approval, unless the proposed change, test or experiment involves a change in the technical specifications incorporated in the license or an unreviewed safety question.

(2) A proposed change, test, or experiment shall be deemed to involve an unreviewed safety question (i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or (ii) if a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report may be created; or (iii) if the margin of safety as defined in the basis for any technical specification is reduced.

(b)(1) The licensee shall maintain records of changes in the facility and of changes in procedures made pursuant to this section, to the extent that these changes constitute changes in the facility as described in the safety analysis report or to the extent that they constitute changes in procedures as described in the safety analysis report. The licensee shall also maintain records of tests and experiments carried out pursuant to paragraph (a) of this section. These records must include a written safety evaluation which provides the bases for the determination that the change, test, or experiment does not involve an unreviewed safety question.

(2) The licensee shall submit, as specified in § 50.4, a report containing a brief description of any changes, tests and experiments, including a summary of the safety evaluation of each. The report may be submitted annually or along with the FSAR [Final Safety

Analysis Report] updates as required by § 50.71(e), or at such shorter intervals as may be specified in the license.

(3) The records of changes in the facility shall be maintained until the date of termination of the license, and records of changes in procedures and records of tests and experiments shall be maintained for a period of five years.

(c) The holder of a license authorizing operation of a production or utilization facility who desires (1) a change in technical specifications or (2) to make a change in the facility or the procedures described in the safety analysis report or to conduct tests or experiments not described in the safety analysis report, which involve an unreviewed safety question or a change in technical specifications, shall submit an application of amendment of his license pursuant to § 50.90.

APPENDIX F

Digital Instrumentation and Control System Features

In the Phase 1 report of this study (NRC, 1995), the committee noted that care must be exercised to take into account inherent characteristics of digital systems and the effect of these characteristics on the processes with which the digital systems interface. Key characteristics of the digital systems include real-time processing, data communications, sequential operation, multiplexing, multitasking, memory sharing, and diverse data transmission and storage media, each of which is discussed below.

REAL-TIME PROCESSING

Real-time systems are defined as those systems in which the correctness of the system response depends not only on the logical results of the computation but also on the time at which the results are produced (Stankovic and Ramamrithan, 1988). A typical real-time system includes a controlling system and a controlled system. The controlling system periodically receives and processes information about the controlled system and the environment and generates control commands in response to this information, which are applied to the controlled system. For this operation to be stable and meet performance requirements, the timing relationship between the controlling system and the controlled system must be such that the complete control sequence (parameter sampling, transmission process, control command generation, and control command transmission back to the process) must be faster than the response time of the controlled process. For critical systems, timing analysis of the controlling system typically considers the worst (rather than average) values for communication delays and execution time. Such worst case analysis often places important constraints on the design to ensure that timing bounds can be met. Such constraints include the use of a special-purpose real-time operating system kernel, nonpreemptive scheduling, and simple data and control flow structures in order to reduce the unpredictability of the response. Interrupts are frequently disabled or are anticipated in the schedule and handled expediently. Real-time systems, because they must provide guaranteed response in the worst case, are typically underutilized when analyzed for average behavior.

Failure modes of real-time systems include the typical failure modes of the controlling system, augmented by timing failures. A timing failure occurs when a deadline is missed. The result of a missed deadline depends on the controlled process. In some cases, a real-time system may tolerate missing several consecutive deadlines if the output parameters are held steady. However, there is often a hard limit to the number of missed deadlines that can be tolerated.

In large applications such as power plants, the real-time processing systems are usually not written from scratch using general-purpose computers. Rather, many vendors offer off-the-shelf systems, and these are widely used in distributed control systems in industrial applications (see, e.g., Sudduth, 1995). As a result, real-time distributed computer systems designed for industrial process control are often a collection of microprocessor-based modules interconnected through a communication network, which execute well-defined process control functions. Function modules are provided for data acquisition, control of process variables, operator communication, and supervisory functions. Programming of such commercially available process control systems often involves the selection and interconnection of functional blocks from a library of modules. Usually this interaction is programmed by the system designer using a graphic interface. Many potential problems associated with constructing real-time systems from scratch are avoided or minimized by restrictions enforced by the use of these special-purpose process control systems. For example, they often rely on the predefined standard function modules, rather than requiring custom programming in general-purpose software languages. This, plus the use of a real-time operating system kernel (e.g., effects of cache memory), simplifies the task of timing analysis and helps ensure predictability. Hardware execution time variation is also an issue that must be addressed. Of course, this does not eliminate all the potential problems (e.g., software quality assurance).

DATA COMMUNICATIONS

A distributed process-control system requires a reliable communication network to link the control nodes together. Reliable communication systems must provide a guaranteed level of performance, even when heavily loaded, and must be able to detect and recover when a message is lost or erroneous. The critical nature of the communication system has led to the development of architectures (and associated protocols) for data-highway communication networks for distributed process-control systems. In a data-highway-based communication system there is a data-link level but no higher level of ISO network protocols (Schoeffler, 1984). Architectures vary throughout the industry, but three types are common: the token passing ring-based, broadcast-based, and cluster-based systems. Well-defined architectures and algorithms for reliable communication have been developed for each type of communication network (Jalote, 1994).

Failure modes associated with communication systems include (a) lost and late messages; (b) misdirected messages; (c) messages that lose meaning after being sent because the sending processor rolls back to a previously saved checkpoint owing to an error (commonly known as orphan messages; see Jalote, 1994); and (d) inconsistent messages to other processes, which can cause the receivers to act inconsistently (commonly known as Byzantine messages; see Lamport et al., 1982).

Failure modes associated with shared resources must also be considered. Multiplexers that sample and combine the data at the transmitting end and multiplexers that decode the signals at the receiving end represent points of vulnerability in the system because multiple signals are sequentially processed by these devices.

SEQUENTIAL OPERATION

Microprocessors in digital instrumentation and control (I&C) systems execute all software commands sequentially. This sequential operation must be considered in addressing the timing and scheduling considerations discussed above. Implications of sequential operations include:

1. The sequential processing capacity of the modules in a control loop needs to be such that loop control response is several times faster than process response time. This is based on closed-loop control stability theory. Although this requirement applies to all control systems, it must be carefully considered in digital control loops. In digital systems additional delays may occur because of interrupts or preemptions of a higher priority. As a result, closed-loop control algorithms should be implemented so that they are executed in a predictable manner, without timing uncertainties introduced by unpredictable interruptions or preemptions.
2. The use of dedicated and separate buses for closed-loop control, for control and alarm operator interfaces, and for performance calculations is highly desirable. This approach reduces the introduction of unnecessary delays into the control loops.

MULTIPLEXING

Digital systems have the capability of sampling multiple plant process parameters and then bringing the sampled data sequentially into digital memory over a single physical communication channel. Similarly, digital systems have the capability of transmitting multiple command control signals to plant processes one at a time over a single channel. Although "multiplexing" is a term that has traditionally been applied to the transmission of these types of process parameter signals, communication links in digital I&C systems also carry multiplexed information of a broader nature, such as performance analysis results, historical data files, and display data files. These multiplexing capabilities introduce common paths in the transmission of information. Also, the multiplexers are themselves sequential devices, which must be considered in addressing the timing and scheduling considerations and the communications considerations discussed previously.

Multiplexing must be coordinated throughout the plant so that all data are acquired and used in a consistent way. Multiplexing of time-sensitive data critical to plant performance or protection against hazards is best handled via deterministic data buses or data links, which handle data in a predictable manner that is easy to verify and validate in design reviews and testing.

Most importantly, multiplexing of independent channels, such as those used in safety systems, must be avoided since it would destroy their independence. Good guidance on this subject is provided in NUREG/CR-6082, Data Communications.

MULTITASKING

Multitasking involves the ability to interrupt a task in progress and initiate or resume a different task that needs to be performed on a higher priority. It is actually a feature of the software but it can affect the performance of a digital system and needs to be accounted for. Multitasking must be considered in addressing the timing and scheduling considerations discussed above.

In time-sensitive applications, preemptive multitasking is not desirable as it may introduce uncertain delays. In this case, handling tasks in a deterministic manner is preferred, so that critical tasks are always scheduled and performed in a predictable manner.

Multitasking is more generally acceptable in functions that are not time-sensitive and do not interfere with time-sensitive functions. For example, multitasking may be useful in off-line functions such as historical data trending analysis or diagnostics calculations.

MEMORY SHARING

Digital systems make use of historical data values to perform control actions, to make performance calculations, and to generate displays. These data are stored so that the data may be accessible to multiple processors. One processor may deposit in memory data sampled from a plant process while other processors use these stored data for other functions. For example, the level of water in a tank may be periodically sampled and stored in memory by one processor while a second processor uses the stored value to vary the opening of a drain valve that regulates water level. A third processor may use the same stored value to start a transfer of water to another tank, and a fourth processor may use it to display the level in the control room.

Memory sharing introduces the need to manage and protect the flow of data in and out of shared memories so that data are valid and consistent at all times. This is a complex subject and there is an extensive literature that should be consulted (see, e.g., Suri et al., 1995; Tannenbaum, 1995; and Jalote, 1994). The impact of memory sharing also must be considered in addressing timing and scheduling considerations.

DIVERSE DATA TRANSMISSION AND STORAGE MEDIA

Digital signals can be stored and can travel on media that are different from those used in analog systems. For example, data may be stored on different types of magnetic media or transmitted over optical data highways. The important differences, both pro and con, need to be recognized.

For example, optical signal transmission media are often used in digital systems. Optical media are more robust than traditional electric conductors. Optical media are immune to all forms of electromagnetic interference and eliminate problems introduced by ground loops in electric circuits. Optical cable offers complete electrical isolation and is resistant to most chemicals. It also generates relatively low noise and produces low signal attenuation. However, the installation of optical fiber cable requires special training and tools.

The use of diverse transmission and storage media in digital I&C systems does not present insurmountable challenges. The media must be environmentally qualified in a manner similar to that in which analog and digital equipment has been qualified in the past.

REFERENCES

Jalote, P. 1994. Fault Tolerance in Distributed Systems. Upper Saddle River, N.J.: Prentice-Hall.

Lamport, L., R. Shostak, and M. Pease. 1982. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems 4(3):382–401.

NRC (National Research Council). 1995. Digital Instrumentation and Control Systems in Nuclear Power Plant Operations and Safety: Safety and Reliability Issues, Phase 1. Board on Energy and Environmental Systems, National Research Council. Washington, D.C.: National Academy Press.

Schoeffler, J.D. 1984. Distributed computer systems for industrial process control. IEEE Computer 17(2):11–18.

Stankovic, J., and K. Ramamrithan. 1988. Tutorial: Hard Real-Time Systems. Los Alamitos, Calif.: IEEE Computer Society Press.

Sudduth, A.1995. Presentation to the committee, Washington, D.C., December.

Suri, N., C.J. Walter, and M.M. Hugue. 1995. Advances in Ultra-Dependable Distributed Systems. Los Alamitos, Calif.: IEEE Computer Society Press.

Tannenbaum, A. 1995. Distributed Operating Systems. Upper Saddle River, N.J.: Prentice-Hall.

Glossary

Analog technology A device in which data are represented by a continuously variable quantity.

Code of Federal Regulations (10 CFR 50, 10 CFR 50.59, 10 CFR 50.90) The Code of Federal Regulations, Title 10, Part 50, governs the licensing of domestic nuclear power plants. Section 50.59 sets forth criteria for determining whether changes to a licensed nuclear power plant require prior USNRC approval. Appendix A of 10 CFR 50 lists "general design criteria" to be followed in the design, construction, and operations of nuclear power plants.

Combinational logic A Boolean algebraic function whose output value is determined by the present conditions (or current inputs), i.e., there is no "state" or memory.

Common-cause failure Multiple component failures having the same cause.

Common-mode failure The failure of multiple components in the same way. Both common-cause and common-mode failures arise when the assumption of independence of the failures of the components is violated. Common-mode failures are a concern when the failures occur concurrently or at least sequentially in a time frame before the minimum number of component is recovered.

Common-mode software failure Failure of redundant sets of software in the same way.

Configuration control/management A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements (ANSI/IEEE 610.12-1990).

Dedication The qualification process performed on commercial-grade items proposed for use in safety systems to assure an equivalent level of quality as obtained for components developed and produced under the formal quality programs of Title 10 CFR Part 50, Appendix B.

Defense-in-depth The conservative design approach that uses multiple, layered systems to provide alternate means of accomplishing different functions related to common goals. This approach provides added protection against natural phenomena and plant operational transients and accidents.

Design basis Information on plant functional components and their response to a set of postulated failure scenarios.

Design faults (vs. random faults) Design faults are those committed during the original design or during subsequent modifications and cause the system that is actually implemented to be different from that which was intended. Design faults can be contrasted with physical faults (sometimes called random faults) which occur during operation, caused by internal or external physical phenomena (wear-out, electromagnetic perturbations, temperature, vibration, etc.).

Digital (technology) A device in which data are represented by a combination of discrete digits, such as 0's and 1's.

Diversity The use of two or more mutually exclusive means of performing the same function. This includes design, functional, and "nameplate" diversity. Design diversity is the use of two or more components with a different internal design to accomplish the same function. Functional diversity is the use of two or more components to achieve different component functions, although the functions may be related in terms of higher-level functions and requirements. Nameplate diversity is the use of components from different manufacturers to accomplish the same function.

Engineered safety features actuation system A set of plant components that work with the reactor protection system to initiate rapid and complete response actions in response to plant transients and accidents.

Environmental qualification A set of testing and certification procedures to assure the operation of nuclear components in anticipated environmental conditions.

Formal methods The use of specifications with mathematically defined semantics and mathematical analysis techniques defined for these specifications.

Generic Letter (95-02) Guidance from the USNRC on review of digital I&C upgrades based on an endorsement of EPRI TR-102348, "Guideline on Licensing Digital Upgrades."

Graded approach Tailoring of review process and resources based on the safety significance of the proposed action.

Hazard analysis A structured process for analyzing a system to identify potential hazards and their root causes.

Human-machine interface (also called human-system interface and human-computer interface). For the purposes of this report, the interactions of plant personnel with the digital I&C system, including the effects of computer displays, plant operations, and I&C maintenance.

Independence Noninteracting or noninterfering components. A set of components has "statistical independence" when the joint probability of a compound event among the set of components equals the product of the probabilities of the individual events that make up the compound event.

Instrumentation and control Systems that provide plant monitoring, control, and protection functions in nuclear power plants.

Mean time between failures A statistical estimation of the average time between failures.

Memory sharing The use of common memory storage for different functions that use a common historical data base.

Multiplexing Transmission of data signals across shared pathways. A multiplexer is a digital switch, connecting data from one of many sources to its output.

Multitasking "Simultaneous" execution of several tasks (processes) on a single computer processor. The operating system controls the switching between the different tasks.

N-version programming The development of different versions of a software program to achieve the same function by different design teams in an effort to achieve fault tolerance.

Probabilistic (risk) assessment method An analysis method used to (a) assess the relative frequency and consequences of postulated events, (b) search for design weaknesses, and (c) identify and assess the frequency and associated risk of improbable events which are beyond the plant design basis.

Reactor protection system A set of plant components that initiate rapid and complete response actions in response to plant transients and accidents to bring the reactor to a safe condition.

Redundancy The use of identical or diverse items to provide alternate means of performing a required function in the event of failure of an individual item. Redundancy is used primarily as defense against "random" or wear-out failures when no diversity is provided.

Safety analysis report The formal documentation of the basis for licensing a nuclear power plant.

Safety-critical application Systems whose failure or malfunction could cause or contribute to an accident.

Safety margin assessment Assessment of (a set of) design criteria relative to known failure criteria.

Safety (and nonsafety) systems Those systems relied upon to remain functioning during and following design basis events to ensure (a) the integrity of the reactor coolant pressure boundary, (b) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (c) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10 CFR 100 guidelines (IEEE 603-1991).

Separation Physical or functional independence of systems.

Sequential logic A Boolean algebraic function whose output value is determined from the current inputs as well as the current "state" which is typically stored in memory elements or delay-inducing feedback loops.

Software quality assurance Development processes and standards that attempt to produce software with certain specified qualities.

Software specification A description of a piece of software which is a basis for its design and implementation.

Standard Review Plan (and Branch Technical Positions, Regulatory Guides) A set of guidance for USNRC reviewers as to what is needed from the licensee to assess the adequacy of a proposed design or what represents a satisfactory method of complying with the licensing requirements. Branch technical positions, regulatory guides, and industry standards provide additional, more detailed guidance.

Static analysis Either manual or automated analysis of software source code to detect potential errors without executing the code.

Thread audit A software code review procedure that traces a particular software program function from input to output.

Unreviewed safety question A failure mode not previously analyzed in a plant's safety analysis report.

Verification and validation Verification is the process of determining whether or not the product of each stage of the system design process fulfills the requirements imposed by the previous design stage. Validation is the test and evaluation of the integrated system design to ensure compliance with the functional, performance, and interface requirements as specified in the system functional requirements (IEEE 7-4.3.2 and IEC 880).