



NASA-CR-198566

International Technology Research Institute



ITRI

WTEC Monograph on

Instrumentation, Control and Safety Systems of Canadian Nuclear Facilities

N95-71514

Unclassified

29/73 0049778

Robert E. Uhrig
Richard J. Carter

July 1993

(NASA-CR-198566) WTEC MONOGRAPH ON
INSTRUMENTATION, CONTROL AND SAFETY
SYSTEMS OF CANADIAN NUCLEAR
FACILITIES (Loyola Coll.) 40 p



International Technology Research Institute
JTEC/WTEC Program
Loyola College in Maryland
4501 North Charles Street
Baltimore, Maryland 21210-2699

ECOLOGY EVALUATION CENTER

WORLD TECHN

ation Center (WTEC) is a companion to the long-established
ation Center (JTEC) at Loyola College. WTEC is operated
o provide assessments of European and Canadian research
selected technologies. The National Science Foundation
agency. Paul Herer, Senior Advisor for Planning and
NSF Program Director for the project. Other sponsors of
National Aeronautics and Space Administration (NASA), the
DOC), the Department of Energy (DOE), the Office of Naval
Advanced Research Projects Agency (DARPA), and the

European market system and the pressures of competition high technology have stimulated the consolidation of companies and nations. The resulting trends are for faster paced development directly competitive with those in the U.S. As European become leaders in research in targeted technologies, it is important that U.S. researchers have access to the results. WTEC provides the important opportunity for U.S. researchers to learn about the accomplishments of their European counterparts. These accomplishments are also of interest in formulating governmental research

med by panels of about six U.S. technical experts. Panelies in the field, technically active, and knowledgeable about research programs. Each panelist spends about one month of taking assessments, and writing reports on a part-time basis. Panels conduct extensive tours of university and industrial foreign host countries. To provide a balanced perspective, industry, academia, and government.

s is on the status and long-term direction of foreign R&D in the United States. Other important aspects include the identification of key researchers, R&D organizations,

ented to workshops where invited participants critique the reports are distributed by the National Technical Information Service, 555 Geary Road, Springfield, Virginia 22161 (703-487-4650). The final findings in papers and books. All results are unclassified.

ff at Loyola College is to coordinate excellent assessments
e highest professional quality. WTEC helps select topics,
organizes tours of foreign laboratories and industrial sites,
workshop presentations, and provides editorial assistance

SPONSOR

The World Technology Evaluation Center, Japanese Technology Evaluation for the Federal Government, and development (R&D) in NSF is the lead support agency for WTEC. Technology Evaluation, is part of WTEC and JTEC include the Department of Commerce (NIST), Research (ONR), the Defense Department, and the U.S. Air Force.

PURPOSE

The steady integration of the best technologies from worldwide sources in European R&D among competing nations and corporations becomes essential that the United States take the first step in the process by a lead in other nations. WTEC findings and trade policies.

APPROACH

The assessments are performed by members of the panel who are leading authorities in both U.S. and foreign research. The effort involves an extensive review of literature, mostly over a twelve-month period. The research facilities in selected countries are visited, and panelists are selected from

ASSESSMENTS

The focus of the assessment efforts relative to those of evolution of the technology and funding sources.

REPORTS

The panel findings are presented as preliminary results. Final reports will be available from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. Panelists also present techniques and public.

**LOYOLA
COLLEGE**

The function of the WTEC staff is to produce reports of the study, recruits experts as panelists, assists in the preparation of the reports, and for the final report.

Mr. Geoff Holdridge
JTEC/WTEC Staff Director
Loyola College
Baltimore, MD 21210

**Dr. George Gamota
Senior Advisor
to JTEC/WTEC
Mitre Corporation
Bedford, MA 01730**

**Dr. Michael J. DeHaemer
Principal Investigator
Loyola College
Baltimore, MD 21210**

WTEC Monograph on

**INSTRUMENTATION, CONTROL AND SAFETY SYSTEMS
OF CANADIAN NUCLEAR FACILITIES**

July 1993

Robert E. Uhrig

Oak Ridge National Laboratory, Oak Ridge, TN
The University of Tennessee, Knoxville, TN

Richard J. Carter

Oak Ridge National Laboratory, Oak Ridge, TN

This document was sponsored by the National Science Foundation (NSF) and the Department of Energy under NSF Grant ENG-9111333, awarded to the World Technology Evaluation Center at Loyola College in Maryland. The Government has certain rights in this material. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, the United States Government, the authors' parent institutions, or Loyola College.

ABSTRACT

This report updates a 1989-90 survey of advanced instrumentation and controls (I&C) technologies and associated human factors issues in the U.S. and Canadian nuclear industries carried out by a team from Oak Ridge National Laboratory (Carter and Uhrig 1990). The authors found that the most advanced I&C systems are in the Canadian CANDU plants, where the newest plant (Darlington) has digital systems in almost 100% of its control systems and in over 70% of its plant protection system. Increased emphasis on human factors and cognitive science in modern control rooms has resulted in a reduced work load for the operators and the elimination of many human errors. Automation implemented through digital instrumentation and control is effectively changing the role of the operator to that of a systems manager.

The hypothesis that *properly introducing digital systems increases safety* is supported by the Canadian experience. The performance of these digital systems has been achieved using appropriate quality assurance programs for both hardware and software development. Recent regulatory authority review of the development of safety-critical software has resulted in the creation of isolated software modules with well defined interfaces and more formal structure in the software generation. The ability of digital systems to detect impending failures and initiate a fail-safe action is a significant safety issue that should be of special interest to nuclear utilities and regulatory authorities around the world.

JTEC/WTEC

Michael J. DeHaemer, Principal Investigator, Director
Geoffrey M. Holdridge, Staff Director and JTEC/WTEC Series Editor
Bobby A. Williams, Assistant Director
Yvonne A. Lilley, Senior Secretary
Catrina M. Foley, Secretary
Aminah Batta, Editorial Assistant

International Technology Research Institute at Loyola College

R. D. Shelton, Director

Copyright 1993 by Loyola College in Maryland. The U.S. Government retains a nonexclusive and nontransferable license to exercise all exclusive rights provided by copyright. The ISBN number for this report is 1-883712-24-6. This report is distributed by the National Technical Information Service (NTIS) of the U.S. Department of Commerce as NTIS Report # PB93-218295. Information on ordering from NTIS is available by calling (703) 487-4650.

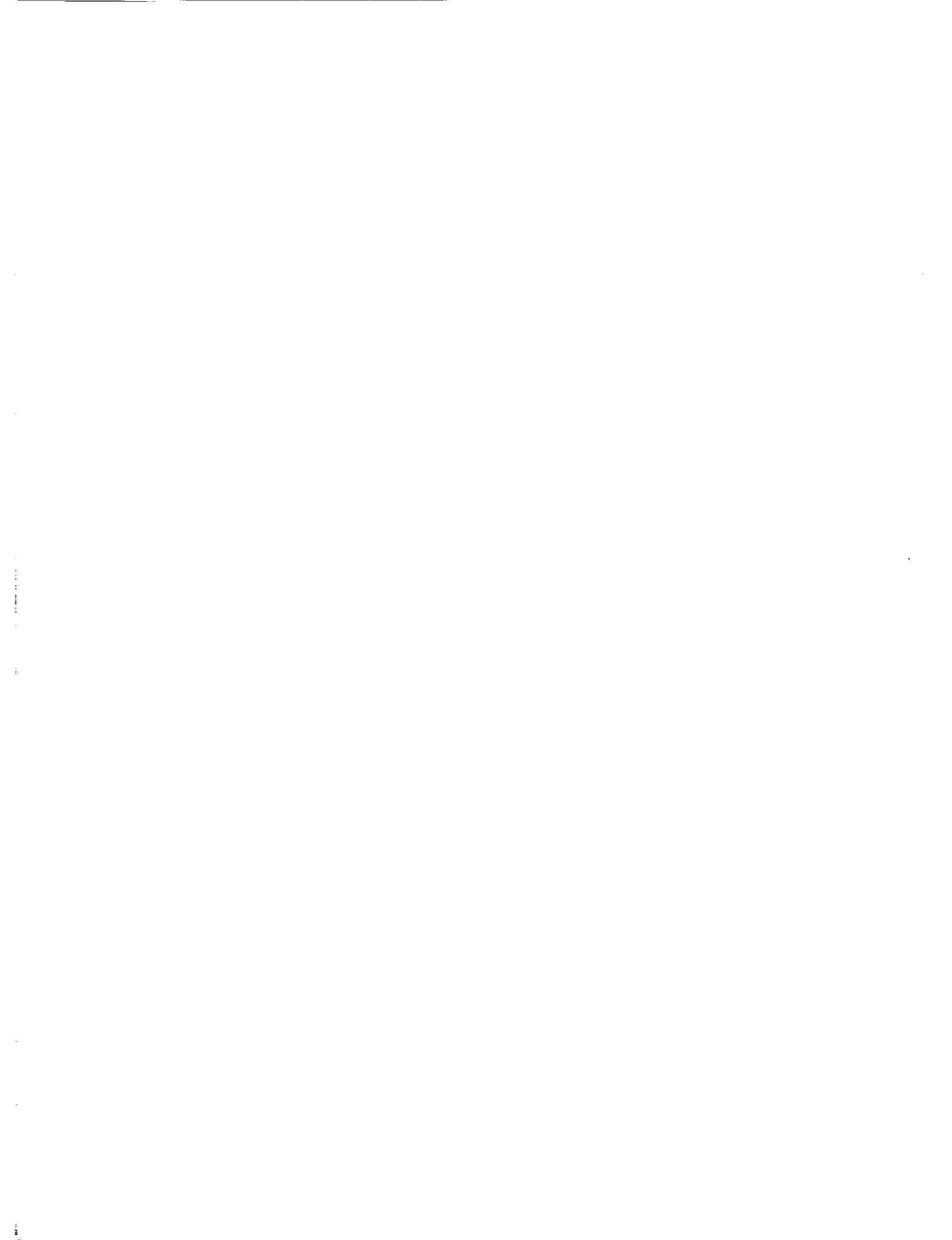


TABLE OF CONTENTS

Table of Contents	1
List of Figures	2
List of Tables	2
Executive Summary and Conclusions	3
Instrumentation, Control and Safety Systems of Canadian Nuclear Facilities	7
Introduction	7
Overview of Nuclear Power Industry in Canada	7
Overview of I&C in Canadian Nuclear Facilities	10
Digital Control Systems	10
Digital Plant Protection Systems	11
CANDU Safety Shutdown System Design	12
Quality Considerations	15
Licensing of Digital I&C and Safety Systems	17
Potential Disadvantages/Adverse Consequences of Advanced I&C	19
Human Factors	20
Human Factors in CANDU Reactors	21
CANDU Personnel	24
Canadian Power Plant Control Rooms	25
CANDU Nuclear Power Plant Control Rooms	25
Features of Modern Canadian Power Plant Control Rooms	26
Control Room for New CANDU Stations	28
Operator's Companion	29

CONTENTS (Continued)

CANDU-3 Digital I&C Safety Systems	30
Plant Display System	30
Distributed Control System	31
Digital Protection Systems	31
Assurance of Adequate Software Quality	32
Safety Implications of CANDU Experience with Digital Systems	32
References	33

LIST OF FIGURES

1. Trend Toward Digital Control and Protection in CANDU Pressurized Heavy Water Reactor Nuclear Steam Supply Systems	4
2. Steam Supply System of a CANDU Reactor	8
3. CANDU-600 SDS-1	13
4. CANDU-600 SDS-2	13

LIST OF TABLES

1. Comparison of Canadian and U.S. Nuclear I&C Systems	6
2. CANDU Nuclear Power Plants in Operation or Under Construction	9
3. Shutdown System Component Failures	11

EXECUTIVE SUMMARY AND CONCLUSIONS

Throughout the world, the nuclear power industry is currently developing advanced control and operator interface systems based on innovative applications of digital computers. Significant changes in the operation of nuclear power plants can be expected from the use of computers for automation and operator aids. Over the past two decades, the Canadian nuclear power plant vendor AECL (Atomic Energy of Canada, Ltd.) and utilities have demonstrated digital instrumentation and control systems to be effective in monitoring and controlling the CANDU (Canada Deuterium-Uranium) nuclear power plants and in providing the degree of safety margin needed to protect both the plant and the public. The Canadian experience of improved performance and increased safety, while using commercial-grade computers and components, has demonstrated a cost-effective approach to the implementation of digital systems in both control and safety systems. The ability of these digital systems to detect impending failures and initiate a fail-safe action is a significant safety issue that should be of special interest to utilities and regulatory authorities around the world.

Canada has by far the most experience in the world with advanced (digital) instrumentation and control (I&C) systems for nuclear power plants. Darlington, the newest CANDU plant, has digital systems in almost 100% of its control systems and over 70% of its plant protection system. The control and plant protection systems use commercial-grade digital components, qualified in much the same way analog components are qualified, plus testing for electromagnetic interference and seismic qualifications. AECL, in plants outside Ontario, has had 36 programmable logic controllers (PLCs¹) in operation in three CANDU plants since 1982 (over 300 system years) with no incidents of spurious plant trips due to any kind of PLC malfunction and no incidence of failure to trip when required. When a digital component or system begins to degrade, the self-checking features immediately put the system in trip mode and alert plant personnel, who in all cases have been able to identify and replace the faulty component within two hours. This performance has been achieved using a software quality assurance program that meets the IEEE and IEC standards, but does not include extraordinary measures to prevent common mode software design errors.

It is very difficult to compare the status of I&C systems in Canadian and U.S. nuclear facilities, because they have developed under very different technical and regulatory environments. The CANDU reactors are large because they use natural uranium. Digital control systems are required to operate at the rated power levels, where

¹ Note: the terms "PLC" (programmable logic controller) and "PDC" (programmable digital controller) are often used interchangeably, depending on the context.

xenon has an influence on the neutron flux distribution and stability. U.S. nuclear reactors use enriched uranium and are substantially smaller. As a result, the influence of xenon on the spatial distribution of the neutron flux is limited, and analog control systems are deemed to be adequate. Necessity and sound engineering have made digital control systems acceptable in the CANDU reactors.

Extensive experience with digital systems in control of early CANDU reactors demonstrated the inherent advantages (reliability, flexibility, stability, etc.). Hence, it was a logical next step to introduce digital systems into safety systems. As a result of Canada's very favorable experience in using digital systems in both control and safety systems, the percent of such systems using digital technology has grown rapidly (see Figure 1). The ability to easily automate many test and calibration functions, to the point of using every other cycle for testing in safety systems, has resulted in significant advantages and safety improvements to the CANDU power plants over plants using analog systems. Indeed, the Canadian use of digital safety systems in nuclear power plants, without analog backup systems, is almost unique in the world.

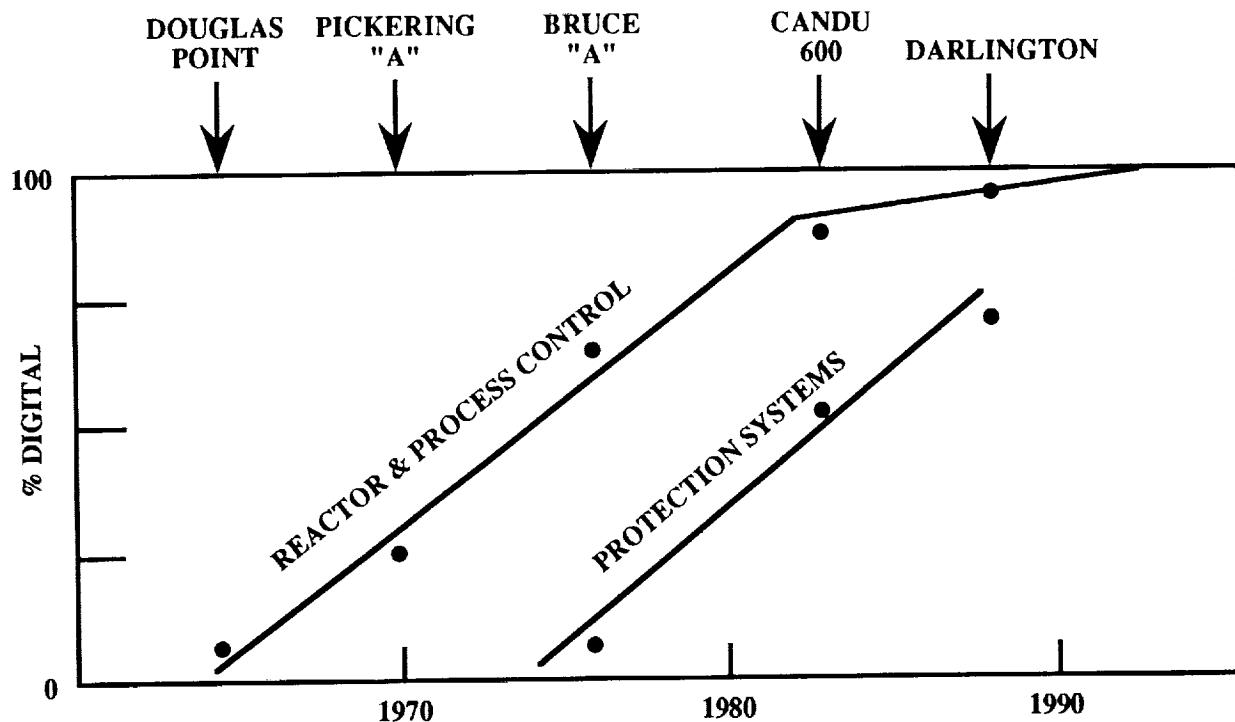


Figure 1. Trend Toward Digital Control and Protection in CANDU Pressurized Heavy Water Reactor Nuclear Steam Supply Systems (PHWR NSSS). (Source: Atomic Energy of Canada, Ltd.)

In the United States, digital control was not originally deemed a necessity to operate nuclear power plants safely, and vendors utilized traditional analog systems for both control and safety. Once the overall design of power plants evolved to a certain level, the rapid growth of the industry (over 100 plants in 25 years) often made regulatory approval of changes difficult. By the time the advantages of digital systems became apparent to U.S. vendors and utilities, they were a decade or more behind the Canadians as far as experience with digital systems was concerned. Although there are exceptions, most U.S. nuclear I&C vendors today utilize digital systems that emulate the function of the analog systems they replace, and make the units *plug compatible*, physically, electronically and functionally.

Table 1 compares I&C systems in U.S. and Canadian nuclear power plants. For the reasons discussed above, the I&C systems in the Canadian plants are well ahead of those in the United States in most categories. Furthermore, there is little expectation that the situation will change significantly in the near future. (However, a recent Electric Power Research Institute (EPRI) initiative could change this situation substantially by the end of the century.) A major contributing cause is that there have been no new orders for nuclear power plants from U.S. utilities since the accident at Three Mile Island. Nevertheless, there is considerable effort being expended in the United States for I&C systems for the next generation of nuclear power plants (SBWR, AP-600, ALWR, and MHTGR). Since many U.S. vendors are associated with foreign vendors (Combustion Engineering is owned by ABB Atom, B&W is 51% owned by Framatom, and General Electric has a very close association with both Toshiba and Hitachi), it is expected that much of the European and Japanese experience in advanced I&C could be available to U.S. vendors for the next generation of nuclear power plants in the United States. Canadian I&C technology is also available in the United States, and AECL is an active competitor in bidding for digital I&C systems (e.g., digital feedwater control systems) in U.S. nuclear plants. AECL has also submitted a letter of intent to the U.S. Nuclear Regulatory Commission to submit the 450 MWe CANDU-3 design for standard design certification under 10 CFR part 52.

The hypothesis that *properly introducing digital systems increases safety* has been supported by the Canadian experience. The safety significance of the performance of digital vs. analog systems is a critically important issue, and it undoubtedly will become more important with aging and obsolescence of hardwired analog components. The use of flexible digital systems permits reallocation of the testing function to the computer, with an attendant increase in reliability and safety. Mounting evidence of the superior performance of digital systems provides a basis for all regulatory authorities to allow utilities worldwide to introduce digital-based systems where it makes sense to do so. The most important step needed for such action is a clear definition by regulatory authorities of the validation and verification requirements and acceptance criteria for both digital hardware and software.

Executive Summary and Conclusions

Table 1
Comparison of Canadian and U.S. Nuclear I&C Systems

	RESEARCH	DEVELOPMENT	IMPLEMENTATION
DIGITAL INSTRUMENTATION	0 →	+ ↗	+ ↗
MAN-MACHINE INTERFACE	0 →	+ ↑	+ ↗
ADVANCED CONTROL	0 →	0 ↗	+ ↗
CONTROL ROOM DESIGN	+ ↗	+ ↗	+ ↗
REGULATORY ACCEPTANCE	+ ↗	+ ↗	+ ↗
ARTIFICIAL INTELLIGENCE	0 →	+ ↗	+ ↗

+ INDICATES THAT CANADA IS CURRENTLY AHEAD

0 INDICATES THAT CANADA AND U.S. ARE CURRENTLY AT THE SAME LEVEL
→ INDICATES THAT CANADA IS PROGRESSING MORE RAPIDLY THAN THE U.S.

↑ INDICATES THAT CANADA AND U.S. ARE PROGRESSING AT THE SAME RATE

INSTRUMENTATION, CONTROL AND SAFETY SYSTEMS OF CANADIAN NUCLEAR FACILITIES

INTRODUCTION

The financial and operational benefits made possible by the use of modern digital monitoring and control in other industries (e.g., petroleum refineries, chemical manufacturing plants, and aircraft systems) have been quite significant, and there is good reason to believe that the benefits to nuclear power plants can be equally attractive. The potential increase in safety resulting from the use of digital systems can provide increased investment protection to the utilities and an increased margin of safety to the regulatory authorities. The point has been reached where the principal licensing issues in using advanced digital systems in nuclear power plants are not hardware reliability or performance, but rather software validity and the interface between humans and systems.

OVERVIEW OF THE NUCLEAR POWER INDUSTRY IN CANADA

The nuclear power industry in Canada is dominated by two organizations: AECL, the only nuclear steam supply system vendor, and Ontario Hydro which operates all but two of the commercial nuclear power plants in Canada (Pt. Lepreau operated by New Brunswick Electric Power Commission, and Gentilly-2 operated by Hydro-Quebec). Ontario Hydro is by far the largest nuclear utility in Canada and operates 20 pressurized heavy-water reactors of the CANDU type at three sites, eight at Pickering, eight at Bruce, and four at Darlington. The nuclear steam supply systems and primary systems at Pickering and Bruce were designed and built by AECL. The steam supply system of a typical CANDU plant is shown in Figure 2. Development of the secondary systems, control design, and construction of the facilities were the responsibility of Ontario Hydro. At Darlington, Ontario Hydro had the primary responsibility for most design and construction aspects of the plant with some assistance in certain areas (e.g., the shut down system) from AECL.

Ontario Hydro is a quasi-governmental utility that has many of the features of the Tennessee Valley Authority in that it has official responsibilities beyond the generation and distribution of electrical power. In addition to providing electrical power to the Province of Ontario from hydro, fossil, and nuclear plants, it is responsible for developing new technology and transferring it to Canadian industry for applications and commercialization. Some of this technological development involves advanced (digital) instrumentation and control associated with the CANDU nuclear plants.

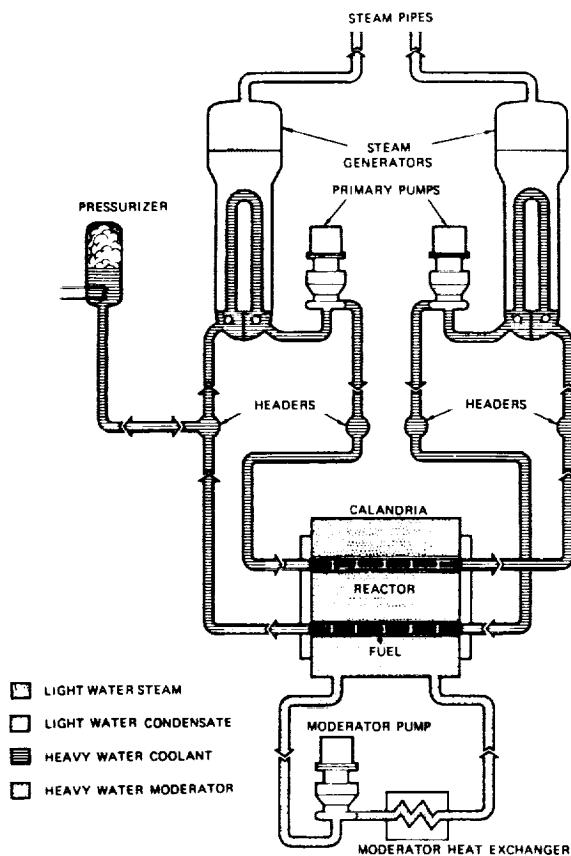


Figure 2. Steam Supply System of a CANDU Reactor. (Lepp and Watkins 1982)

AECL is a "Crown Corporation" charged with operation of the Chalk River facility near Pembroke, Ontario and the Whiteshell facility near Pinawa, Manitoba for the Canadian government, as well as exploitation and commercialization of CANDU nuclear power plants and associated technologies. AECL designs and markets the CANDU pressure tube reactor and associated control rooms. For many years AECL has developed and applied computer/digital technology for both process and reactivity control of nuclear power stations. The first AECL digital control system was implemented in the mid-1960s. AECL has also applied this technology to fossil-fueled plants.

AECL has had the primary responsibility for major systems of the CANDU plants built by all CANDU owners, including those built by Ontario Hydro, and has exclusive overseas rights to the CANDU technology. Currently, AECL is building several 700 megawatt electric (MWe) plants in Romania and Korea, and has undertaken the detailed design of a 450 MWe advanced "CANDU-3" plant for the 1990s.

There are 32 CANDU nuclear power plants in operation or under construction throughout the world in addition to three smaller demonstration plants (Douglas Point, Gentilly-1, and NPD), which have been decommissioned. These plants are listed in Table 2. Twenty of these plants are owned by Ontario Hydro, which has accumulated the vast majority of the experience in their operation. Both Ontario Hydro and AECL have been very active in the development and implementation of the I&C systems of the CANDU reactors. Since this report is intended to convey the overall picture of the Canadian experience with advanced instrumentation and control systems, no attempt has been made to identify the individual contributions of Ontario Hydro and AECL.

Table 2
CANDU Nuclear Power Plants in Operation or Under Construction

Plant Country	No. of Units	Power MWe	Operational Start Dates	Owner or Country
Pickering-A	4	504	1971-1973	Ontario Hydro
Pickering-B	4	504	1982-1986	Ontario Hydro
Bruce-A	4	885	1977-1979	Ontario Hydro
Bruce-B	4	905	1984-1987	Ontario Hydro
Pt. Lepreau	1	680	1982	New Brunswick Power
Gentilly-2	1	685	1982	Hydro-Quebec
Wolsong*	1	679	1982	Korea
Embalse	1	648	1983	Argentina
Darlington-A	4	884	1989-1992	Ontario Hydro
Cernavoda	5	705	1995-1999	Romania
Rapp**	2	220	1971, 1980	India
Kanupp**	1	137	1971	Pakistan

* AECL has a contract for Wolsong-2 for operation late in 1997. A letter of intent for two more CANDU plants at Wolsong was recently announced.

** These units were designed by the Canadian General Electric Company. Hence, the comments on CANDU control and safety systems in this report do not apply.

All CANDU plants use heavy water for neutron moderation and cooling. The coolant is kept in liquid form by pressurization in horizontal pressure tubes that hold the fuel and are surrounded by the heavy water moderator at low pressure and temperature. The core region is contained in a large horizontal cylindrical calandria. All units operate with natural uranium fuel and utilize on-line refueling to keep the inventories of fissionable material and fission products at appropriate levels, thereby maintaining adequate reactivity for power maneuvering and overcoming xenon poisoning.

OVERVIEW OF I&C IN CANADIAN NUCLEAR FACILITIES

The CANDU design was the first commercial nuclear power plant design to include computers in safety systems, using programmable logic comparators (PLCs). This occurred in CANDU-600 in the early 1980s to implement the trip decision logic for process trip parameters. The trend toward digital control and protection systems in CANDU pressurized heavy-water reactors is clearly shown in Figure 1, which presents an evolving trend from almost no digital control systems in the Douglas Point Plant in 1965 to 100% in the Darlington units that went on-line in 1990. Indeed, the Darlington units, which have 1450 PLCs, are automated to a high degree, including automatic startup from source range to full power, built-in component surveillance, system diagnostics, parameter checking, error logging, and an elaborate data-acquisition system. Digital plant protection systems increased from a few components in the units at the Bruce Station in the late 1970s to about 70% at the Darlington plant. The complete centralized dual digital process control system, including input/output and data communications, was designed for an unavailability of 10^{-2} year/year. It has, in fact, achieved 10^{-3} year/year. The digital control systems of the plants have achieved a 99.8% overall availability factor over 288 reactor-years of operation.

Digital Control Systems

The trend toward digital control is a natural outgrowth of a solution to the problem of controlling a large, multi-region natural uranium core with low excess reactivity. The addition of new fuel required to raise power, plus xenon poisoning at higher power levels, introduces modal variations that threaten the stability of the system. Control of these modal variations in the various regions of the core is feasible only with a digital control system. Experience has demonstrated that the reliability of the digital systems greatly exceeds that of analog systems. Hence it was only logical to introduce fully automated control systems into the Darlington plants.

Distributed control systems (DCSs) are planned for the CANDU Model 3 (450 MWe) and CANDU-9 (900 MWe) plants being designed for domestic use and export, respectively, in the 1990s. The distributed control system will perform signal scanning and control logic functions for most of the process systems used for normal

operation of the plants, while separate systems will be provided for safety functions. The DCS is a programmable logic control system consisting of geographically distributed input/output stations and a number of programmable control processors. The input/output stations and control processors will be linked by data highways. Signal monitoring and operator interface functions will be performed by a separate plant display system, which will be linked to the DCS data highways. The plant display system (PDS) also will perform some operator interface functions for the safety system.

Digital Plant Protection Systems

The trend toward a higher percentage of digital components in the plant protection system again grew out of the CANDU experience of high reliability when digital components were introduced. Spurious trips virtually disappeared, set-point drift was eliminated, calibration was minimized, and the overall reliability of the plant protection system improved dramatically. Digital process and reactor controls plus *stepback* (which, under some conditions, reduces power before trip conditions are reached) have also contributed to the low trip rate.

The hypothesis that *properly introducing digital systems increases safety* is supported by the component failure rates in the computerized shutdown systems of the plant protection system. Table 3 shows the failures over a five-year period (from initial criticality) for the Point Lepreau CANDU-600. All of the 44 failures in the PLCs were hardware wearout failures, and none of them introduced a potentially unsafe situation (i.e., all components failed in a safe state). This is a clear demonstration of the computer's ability to detect anomalies or failures (in both its input data and its own operation) and fail in a safe manner. By contrast, 63 of the 146 conventional component failures (43%) were of potentially unsafe kinds (i.e., they temporarily diminished the overall redundancy of the automatic protection systems).

Table 3
Shutdown System Component Failures
(five-year record at Point Lepreau CANDU Plant)

Type of Equipment	Total Failures	Potentially Unsafe Failures
Programmable Logic Controllers	44	0
Conventional (Analog) Hardware	146	63

Source: (Pauksens et al. 1988)

Since 1982, three CANDU-600 Stations (Wolsong-1, Gentilly-2, and Pt. Lepreau) have a total of 288 PLC-years of operating history without a single potentially unsafe failure reported. In that time, there have been no incidents of spurious plant trips due to any kind of PLC malfunction as well as no incidence of failure to trip when required. All failures have been safe failures compared to about one-fourth of failures in analog systems being potentially unsafe, temporarily reducing the redundancy of protection until corrected. Hence, safety availability (converting potentially unsafe failures into safe failures by tripping the channel) has been enhanced. The self-checking features have detected and alarmed several hardware failures, each of which took less than two hours to identify and repair by appropriate board replacement.

Darlington has fully computerized shutdown systems, including safety trip decision logic and channelized displays to the operator, automated testing, and monitoring. While overall functionality has been increased, the safety-critical portions have been localized to the channelized trip computers and the trip functions kept as simple as possible. Each shutdown system (including the I&C and reactivity devices) has consistently achieved unavailabilities of about 10^{-4} year/year. (The unavailability of a trip computer is limited primarily by the software.) Reactor trip frequency with the reactor critical, during the period after high-power testing and plant shakedown were completed, was 0.75 occurrences/year for both shutdown systems. The fault-tree analysis and the failure modes and effects analysis (FMEA) of the plant protection system both support the goal in the present plant protection system of one failure in 1000 years of operation of a CANDU reactor. The actual unavailability is probably an order of magnitude better than this target.

To illustrate the current status in Canadian I&C systems, a detailed description of the CANDU-3 control and safety systems, including automation (management) of control of the plant, is included later in this report. This system evolved from the CANDU-600 and Darlington designs and benefitted from their experience. Furthermore, the CANDU-3 design has a modern, all-digital control room that integrates many of the control functions while maintaining the benefits of distributed control.

CANDU SAFETY SHUTDOWN SYSTEM DESIGN

The Darlington Nuclear Power Station, which began operation of its Unit #2 in 1990, represents the most modern commercially available system as far as computerized shutdown design is concerned. The major functions of this system include trip of the reactor (if required), computer-assisted testing of safety system components, channelized video display of safety system parameters (eliminating conventional panel meters completely) and on-line monitoring of system operation to immediately detect many equipment malfunctions.

Canadian CANDU reactors are designed with a number of systems to shut down the reactor, maintain cooling of the fuel, and contain radiation releases from the fuel and heat transport system, should an accident occur. Every reactor put into service since 1976 has two totally independent triplicated shutdown systems (called SDS-1 and SDS-2) to meet reliability targets. Each system must be independent of the other (different sensors, different logic, different types of reactivity devices, different software, and even different suppliers when possible), must use diverse designs, and must be physically separated. The Canadian regulatory body for nuclear power, AECB (the Atomic Energy Control Board), has accepted that if the two shutdown systems are diverse, are independent of each other and other process systems, and meet their unavailability goals, it is incredible that both systems would fail coincidentally when called upon to shut down the plant.

SDS-1 uses control rods that drop into the reactor from the top, and SDS-2 injects a gadolinium-nitrate solution into the heavy-water moderator using nozzles that enter the reactor from the side. Figures 3 and 4 are block diagrams of SDS-1 and SDS-2, respectively, for a CANDU-600. Each shutdown system must protect against the same group of design basis accidents, and each design basis accident must be detected by two diverse measurements on each shutdown system. These computers are required to meet a 100 millisecond response time requirement for the shutdown system.

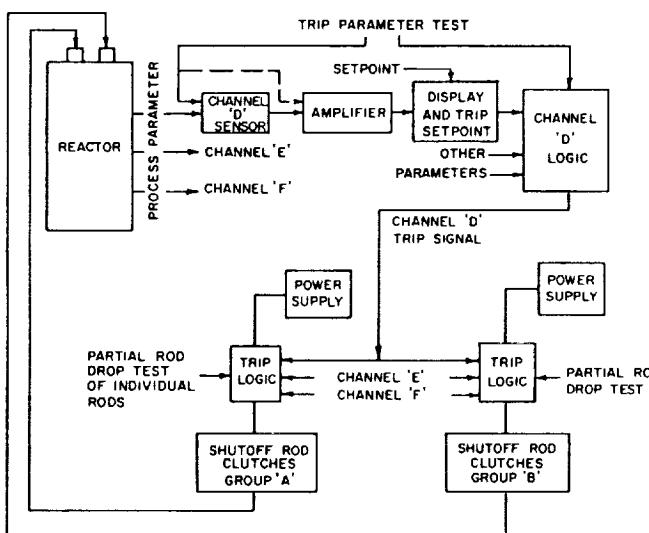


Figure 3. CANDU-600 SDS-1

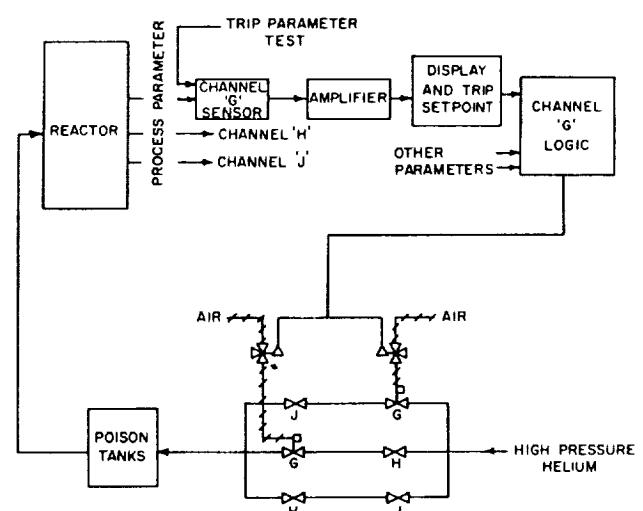


Figure 4. CANDU-600 SDS-2

Source: (Lepp and Watkins 1982)

Both SDS-1 and SDS-2 have hierarchical configurations. The bottom layer of this hierarchy uses six computers (three for SDS-1 and three for SDS-2) and performs the following functions: reads and checks safety system parameters, performs the trip determination algorithm and issues trip signals via digital outputs, performs self-checks, and drives alarm windows on the main control room panels. The system also sends plant parameters and trip computer status information to the display/test computers via the fiber optic link and receives calibration data for in-core, self-powered flux detectors from the display/test computers via the fiber optic link.

The shutdown systems have stringent reliability requirements. For licensing reasons, each system must be unavailable to trip the reactor less than 10^{-3} of the time, and this performance must be confirmed by regular testing. The system has been designed to minimize spurious reactor trips, with a target of less than 0.1 spurious trips per year. The design is based on three identical but physically separate channels in each safety system. Two out of three SDS-1 or SDS-2 channels must trip to cause a reactor trip. This arrangement allows periodic on-line single-channel testing to verify that unavailability targets are being met. It also guarantees that no single random failure will trip the reactor, even during testing. The communications links on each shutdown system are interlocked to ensure that only one channel may be tested or recalibrated at any one time. If a channel is in a tripped state for any reason, the system will not permit testing to take place on another channel, thus preventing spurious reactor trips.

There are four levels of computers in the safety shutdown system. All process and neutronic instruments in a single channel are connected to the trip computer in that channel.

1. Trip Computer. SDS-1 uses general coincidence logic (i.e., any channelized parameter exceeding its setpoint can cause a channel trip). SDS-2 uses local coincidence logic (i.e., a channel will trip only when the same parameter exceeds its setpoint in at least two channels).
2. Display/Test Computers. The next layer up consists of the display/test computers (which are also channelized). They perform the following functions: exchange information with trip and monitor computers, drive two panel-mounted video displays so that the operator can see the values of the process and neutronic trip parameters and their setpoints, and issue test signals to field devices on command from the monitor computers.
3. Shutdown System Monitor Computers. The next layer up is the shutdown system monitor computers, which are not channelized. They perform the various identification and communications functions associated with monitoring. There is only one shutdown system monitor computer per shutdown system.

4. Safety System Monitor Computer. The top layer of the system is the safety system monitor computer. There is only one such computer in the station. It accepts data (e.g., alarm messages and test results) via serial links from all eight shutdown system monitor computers at the Darlington plant (two systems in each of four reactor units). Its function is historical data storage, with the capability to recall raw data off-line.

Experience has shown that from time to time it may become necessary to modify programmed trip setpoints, alter the conditioning logic, or add new trip parameters. Such changes may originate from changing operational considerations or regulatory requirements and analyses. With conventional technology, implementation of all but the simplest of changes can be a serious problem because of the competing demands of safety and power production. If the plant must be shut down to make the changes, a very costly loss of power production may be incurred. If it is kept operating, there can be a significant risk of impaired protection or a costly spurious trip resulting from human error during the installation and testing process. With a computerized shutdown system, much of the modification effort is moved off-line into the software development laboratory, with a significant benefit in reduced outage time and/or reduced system impairment time. In particular, the use of trip computers allows activities equivalent to wiring, calibration, and testing to occur in parallel with plant operation and with no compromise of safety system availability.

QUALITY CONSIDERATIONS

A key to the reliability of the I&C and safety systems of the CANDU plants is a thorough quality assurance program for both hardware and software. In addition, both the software and hardware are kept to the minimum required to carry out the safety functions, thereby minimizing the verification and validation (V&V) required. For example, the PLCs used in the CANDU 600 units have no operating system, no use of interrupts, no keyboard, and no displays other than a light emitting diode (LED) display for fault diagnosis. The software occupies about 3K words of EPROM (electronically programmable read only memory), and it uses a scratchpad of about 100 words of RAM. It is written in assembly language and consists of a single endless loop that calls six modules in turn, taking about 35 ms per pass. The software is designed so that every second pass through the loop is executed with test data instead of real-field inputs. There are ten sets of test data, which are designed to test all significant combinations of inputs and their failures, and for which the self-test module can verify the expected outputs of each trip parameter. Each module is dedicated to one function or one trip parameter. One module computes the estimate of reactor power for conditioning setpoints, the next three compare their process variables to the calculated setpoint, the fifth performs diagnostic self-checks and drives the output contacts, and the sixth and last initializes the PLC for the next pass.

The PLC also performs checksums on all PROMs every 350 ms to guarantee the integrity of the software logic and setpoints. The input/output hardware is tested on each pass by wraparound input/output, and the output signals are changed periodically to permit the software to test for correct operation. Finally, all of these checks are used to determine if the watchdog output should be toggled. The watchdog is a simple AC-coupled device that drops out, opening a contact in the trip logic chain and thus opening the channel if it is not toggled every 100 ms. Hence, stall-type failures of the PLC are also caught.

The hardware, which is composed entirely of commercial-grade components, was qualified in much the same way as analog equipment, plus additional testing appropriate to digital systems such as electromagnetic interference and elevated temperature test. The seismic qualification, which was performed by testing the PLC (the OH 180 model designed by Ontario Hydro and used extensively in CANDU plants) in its cabinet on a shaker table, resulted in some modifications for stiffening and retaining components in receptacles. Shielding was added to reduce the electromagnetic interference. Operation at elevated temperatures demonstrated that no modifications were necessary. The qualification exercise demonstrated that commercial-grade equipment could be qualified to specific industrial requirements in a straightforward manner, and its use can be a cost-effective alternative to equipment specially designed for harsh environments.

Thirty-six PLC systems have been in operation in three CANDU plants since 1982. In that time, there have been no incidents of spurious plant trips due to any kind of PLC malfunction and no incidence of failure to trip when required. The self-checking features have alarmed several hardware failures, each taking less than two hours to identify and repair by appropriate board replacement.

In the case of the Darlington plants, additional steps have been taken to assure the diversity of the systems. For instance, the trip computers for SDS-1 and SDS-2 are from different manufacturers; the two shutdown systems are coded in different higher level languages (Fortran on SDS-1 and Pascal on SDS-2) with some use of assembler language, using independent design teams; SDS-1 software consists of an infinite loop while SDS-2 utilizes a small kernel; watchdog timers are implemented on each trip computer; and self-checking and fail-safe software functions are present but differ from the PLCs.

The safety significance of the PLCs vs. analog systems is a critically important point, and undoubtedly it will become even more definitive with the aging of analog hardwired safety systems. Most plants in the United States have operational safety systems based on analog hardwired components. Periodic testing initiated by humans is the accepted method of detecting failures in such components, but this type of testing is subject to human error. Reallocation of the test function to a computer clearly improves safety. The clear superiority of digital systems, with their

ability to diagnose impending failures and initiate a fail-safe action, is a significant safety issue that should be of special interest to every utility, as well as to all nuclear regulatory authorities.

LICENSING OF DIGITAL I&C AND SAFETY SYSTEMS

In the licensing of the Darlington Plant, the Canadian Atomic Energy Control Board (AECB) raised a number of issues regarding the design of the digital safety systems, primarily questions about the software used in these digital systems. The questions were more philosophical than safety related and dealt with long-term issues rather than an immediate concern with specific problems of the Darlington control and safety systems. The principal issues were:

1. There was no agreed upon measurable definition of acceptability for the engineering of safety-critical software,
2. There were no widely accepted and adopted practices for the specification, design verification and testing of safety-critical software in existence,
3. It was not possible to quantify the achieved reliability of the software component of the safety system,
4. It was not possible to quantify the benefits of using diverse software, and
5. It was not possible to exhaustively test software in all of its possible modes; thus it was unclear what constitutes a sufficient degree of testing.

AECL and Ontario Hydro were required to backfit several additional design and verification processes (after the original software development process was completed).

The application of many of these techniques represented their first use in a nuclear safety-critical application. These included:

1. Preparation of a mathematically precise software requirements specification,
2. Formal verification of the code against the requirements specification,
3. Carrying out of statistically significant trajectory-based random testing to demonstrate that the software reliability was consistent with the system reliability requirement, and

4. Preparation of a hazard analysis of the code to identify failure modes that may lead to an unsafe event.

To avoid similar difficulties and to assure that these techniques were applied *during* (not after) the development of the software, Ontario Hydro and AECL jointly formulated a strategy for the development of a set of standards, procedures and guidelines for software engineering to address these requirements for all levels of criticality. The result is a high-level "Standard for the Software Engineering of Safety-Critical Software" that defines the software engineering process, the outputs from the process, and the requirements to be met by each output. The requirements are expressed in methodology-independent terms so that various techniques for software engineering may be used to meet the requirements of the standard. This allows the standard to be used to assess the acceptability of the various proposed techniques and allows for techniques to evolve without requiring changes to the standard.

Equally important is the increased modularization of the software so that modules that have undergone the comprehensive review processes described above, and that have been documented and tested in plants, can be reused. The prospect that a module can be reused in other plants is an additional incentive for the vendor and/or the utility to make the investment necessary to assure that the software is error-free. This also limits the additional V&V needed to the interfaces between modules when changes in the software are made only by adding, deleting or substituting modules that have previously been subjected to rigorous V&V.

The design and review process needed for licensing of digital systems is still evolving as discussions continue among AECL, Ontario Hydro and the AECB. Two design methodologies currently appear to offer the most promise. These are:

1. The Rational Design Process, a mathematically rigorous approach that documents a deterministic relationship between the pre- and post-conditions of all the inputs and outputs of the software, and
2. The Integrated Approach, a graphical function block methodology that has undergone less scrutiny by the AECB but has advantages in terms of reviewability, re-use of software modules, flexibility, and cost effectiveness.

The Rational Design Process is being used in the Darlington redesign process. There are indications that software reviewability and simplicity contributes more to safety than proof of correctness, but additional R&D is needed to demonstrate this hypothesis. If this hypothesis can be demonstrated, the Integrated Approach methodology may be better.

There is no international consensus on what constitutes adequate safety-critical software design requirements. AECL has accepted an independent review panel

appointed by the International Atomic Energy Agency (IAEA) to review the software design of the Wolsong-2 project. German, French and Japanese plants that have digital safety systems require hardwired analog systems as backups. The only digital systems in current U.S. plants are "plug compatible" direct substitutes for analog systems, and serious review of proposed digital I&C and safety systems for advanced plants (AP-600, SBWR, etc.) are only beginning.

The description of the development of software in accordance with the Standard for Software Engineering of Safety-Critical Software is well beyond the scope of this report. Suffice to say that it involves many of the following:

1. Planned and systematic procedures to be followed during the development of the software and over the lifetime of the plant,
2. Comprehensive documentation of the process expressed in mathematical terms,
3. Mathematical verification to demonstrate compliance with specifications, both systematic and random testing,
4. Configuration management over any changes in either the software or hardware,
5. Maintaining independence of design and verification personnel, and
6. Performance of analyses to identify and evaluate potential safety hazards associated with the computer system.

It is clear that AECL and Ontario Hydro are at the forefront of the development of standards for software engineering of safety-critical software.

POTENTIAL DISADVANTAGES/ADVERSE CONSEQUENCES OF ADVANCED I&C

The advantages of introducing advanced digital systems into nuclear power plants, especially in view of the Canadian experience, appear to be overwhelming. Indeed, a compelling case can be made that safety is increased by the introduction of digital systems. This, of course, is dependent upon the digital systems working properly all the time. Unfortunately, this may not be the case. All digital systems, even the most elementary systems such as PLCs, rely on some sort of software (that may be implemented in hardware such as EPROMs) to enable the system to carry out the desired function. Operating systems have been found to have software errors after several years of extensive use in the field. Numerous errors have even been found in the operating system of computers. A Canadian firm manufacturing a cancer treatment radiation device had a disastrous experience with a software error in a digital control system that resulted in the death of two patients and over-exposure

of several others. As tragic as this was, it pales in the light of what potentially could have happened if that defective digital system were in a nuclear power plant and all safety and backup systems failed or were disabled (as in the Chernobyl accident).

Although Canadian designers target very high availability in their digital systems, they do not presume that there will not be failures. Proper system design considerations (including "defense in depth") can mitigate the impact of failures. Further, it is realized that software errors are design faults as opposed to wear-out faults more prevalent in conventional analog systems (which can also contain design faults). The key used by Canadian designers to reduce design faults to an acceptable level is management of system complexity.

The potential for software errors drives home the absolute necessity for a thorough and effective quality control program that incorporates verification and validation throughout the software development process for safety-grade systems. The Canadians incrementally introduced digital systems into their plants over almost two decades. Even so, the startup of the first Darlington plant was held up for many months by the Canadian regulatory authorities to assure that the software used in the plant protection system had been subjected to adequate quality assurance.

The cost of an adequate software quality assurance program can be staggering if there is no consensus among utilities, designers, and regulators establishing achievable, cost-effective V&V and software engineering methodology for safety-critical applications. Even the IEEE 7.4.3.2 standard can be prohibitively expensive to implement for small systems, especially those that are not produced in large quantities. It seems to be an accepted fact that the software for most digital systems will cost more than the hardware.

The trade-off between potential improvements in safety and reliability vs. the potentially adverse (even catastrophic) results of a software error presents a regulatory dilemma that somehow must be resolved. This may require more research into different or improved methods of V&V or alternate approaches to specifying regulatory requirements. The experience with the CANDU plants, where software errors have not been a significant issue over the years, is encouraging. This undoubtedly is due to the thorough V&V program implemented. The recent AECL/Ontario Hydro response to the AECB challenge is leading the way. The challenge is to retain thoroughness while reducing cost.

HUMAN FACTORS

Human factors are being given high priority to improve safety, improve operator performance, reduce workload, and reduce costs associated with human error

throughout the plant life cycle. There are two major thrusts in this program being applied during the design phase of the life cycle. These are as follows:

1. Revision of the plant design and operations processes to incorporate principles and practices established in the academic/technical disciplines of human factors engineering and cognitive science to ensure that human characteristics and behavior are considered. The goals are to reduce the potential for human error, ensure that rigorous design processes are being utilized, and ensure auditability.
2. Effective utilization of new technologies and processes to design a plant human-machine interface that will significantly reduce the incidence of human error, improve operator performance, reduce operator workload, and thereby improve both reliability and safety. Significant event data from operating nuclear plants consistently indicate that human factors issues (in design, operation, maintenance, selection and training of personnel, construction, commissioning and organizational effectiveness) contribute to equipment or safety barrier impairment in 40-60% of the cases.

Human Factors in CANDU Reactors

Human factors requirements for nuclear power plants have not been dictated by the Canadian AECB. However, the Canadian Standards Association (CSA) and the nuclear industry as a whole are sponsoring the development of guidelines. The human factors group at Ontario Hydro currently uses Institute for Nuclear Power Operation guides, NUREG-0700 ("Guidelines for Control Room Reviews"), and MIL-STD-1472 ("Human Engineering Design Criteria for Military Systems, Equipment, and Facilities"). The AECL human factors group is using NUREG-0700, Electric Power Research Institute human factors guidelines (e.g., "Guide to Nuclear Power Plant Control Room Design"), and visual display unit documents developed by the Idaho National Engineering Laboratory during design of the advanced control room of the Advanced Test Reactor. They are continually assessing and evaluating feedback from operating CANDU plants in order to improve the effectiveness of the human role in the control room. It should be noted that there is some doubt as to whether existing human factors guidelines are applicable to advanced instrumentation and controls.

Operator Training. Ontario Hydro operator trainees spend their first two years of employment in training. When students first enter the training program, they do not generally have any previous formal computer training. Training is now conducted at the Eastern Nuclear Training Center for Pickering and Darlington personnel and at the Western Nuclear Training Center for Bruce personnel. Full scope simulators with the unique characteristics of the specific plants have also been installed at all Ontario Hydro sites as well as the Point Lepreau and Gentilly sites. The training comprises both classroom instruction and training in a full-scope simulator.

Operator training for the Darlington control room is also performed by Ontario Hydro and includes training on the Darlington simulator at the Eastern Nuclear Training Center.

Training materials for the later CANDU stations have always contained information on advanced instrumentation, controls and computer generated displays (CGDs). The features of digital controls are routinely discussed during other systems training in order to show system interrelationships. Utilization of advanced instrumentation, controls, and CGDs, along with conventional instrumentation is highly encouraged. The use of digital instrumentation and controls is an integrated part of the overall training program for Darlington. Training also consists of instruction on signal sources, correction factor calculations performed by the computer, and software flow charts.

Instructors at Ontario Hydro's Eastern Nuclear Training Center have indicated that they have not seen any significant differences in the training requirements for digital instrumentation and controls vs. other plant systems. Indeed, they said that it might be easier to teach candidates on advanced systems than on conventional systems. AECL personnel have stated that it was not more difficult to retrain the operators for the modified Courtenay Bay control room (AECL's first modern control room in a fossil plant having only video displays) than it was to train operators for the CANDU control rooms.

Procedures. Traditionally the development of control room procedures had not been started by the Canadian utilities until late in the control room design process. Procedures for existing CANDU power plants include system operating procedures, chemistry control procedures, an abnormal incidents manual, and operating memoranda. Detailed operating procedures, which were developed in parallel with the plant human-machine interface, form the basis for the information system design. Operators are involved during the preparation and checkout of the procedures.

Use of Simulators. AECL has used and is using simulation techniques in engineering and human-machine interface designs of the existing CANDU control rooms, the advanced control room, and control rooms of the future. Part-task simulators and mockups were also utilized during the design of the Courtenay Bay control room. These simulation tools are used during the initial training of the operators and instructors. AECL staff members have stated that there is a growing recognition by the Canadian utility community of the worth of training simulators.

Physical/Cognitive Workload. AECL's goal in using advanced instrumentation and controls technology has been to simplify required operator actions and to relieve the human of mundane, routine, and tedious tasks. It appears that they have been successful in that the Darlington control room requires less manual control than

Pickering B. Ontario Hydro management concurs that the technological changes being made at Darlington will reduce operator workload.

AECL personnel have indicated that the operator's cognitive workload in the advanced control room is significantly lightened compared to earlier CANDU control rooms. The operator "keeps in touch" with the reactor systems via the standard shift turnover tools (i.e., data logging, bar chart recorders, and parameter trend displays). AECL personnel have indicated that procedures response time should be linked to the annunciation system priority structure to have a "cognitive level" of operation for the operator. There is some concern that the cognitive workload should not be decreased too far, because the operator needs a purpose and a sense of accomplishment during general shift work as well as familiarity with the computer system.

Operator Performance. There is a perception among many in the nuclear industry that the operator is the "weak link" in nuclear plant safety. Statistics indicate that 57% of the errors in all CANDU stations have been human related. Through the use of advanced instrumentation and controls technology, operator involvement in routine tasks and in tasks for which the required response is well defined has been minimized. It is the expectation of both AECL and Ontario Hydro that, by doing this, the frequency of control room operator errors has been reduced well below the levels typical in conventionally instrumented pressurized water reactors. The human factors group at Ontario Hydro has conducted a number of time-line studies of the operator in the control room. Their results suggest that the performance of first operators has indeed changed; they now make fewer errors and perform their tasks more quickly than before.

It is too early to tell whether the changes introduced in the Courtenay Bay control room (an oil-fired power plant with a prototype control console that has only video displays) have decreased the incidence of errors, but the operator can now move more easily and naturally between the CGDs. For the control room of the future, AECL is trying to address and deal with knowledge- and rule-based human behavior instead of skill-based behavior. With the use of digital equipment increasing from the earlier generation CANDU plants to Darlington, the first operator's job has become easier and can be performed more efficiently. AECL has indicated that with the introduction of advanced instrumentation and controls, the operator can think instead of running and doing.

Maintenance. Ease of maintenance was considered during development of the digital software for Pickering B, Darlington, and Courtenay Bay. The software was designed to be simple and to permit revision efficiently and with minimal risk. (However, see AECB concerns cited elsewhere in this report.) Ease of access for maintenance of hardware components was considered during design of the Darlington control room. Accessibility for maintenance is also being considered

during design of the advanced control room. Much of the hardware and software will be able to perform self-check, self-diagnosis, and self-test. More components than before will be placed in accessible areas, maintenance methods will be simplified, and ample access and equipment for all required maintenance will be provided.

Intelligent Display of Operating Procedures. Personnel at both Ontario Hydro and AECL have indicated that intelligent display of normal and off-normal operating procedures would be beneficial to control room operators. However, there is concern that current technology is not capable of presenting an intelligent display that meets the operator's needs and that more research remains before this option becomes a reality. A display of critical parameters to monitor during off-normal events would also be helpful. Currently, AECL is working on "context specific" displays to provide overview displays of all pertinent information needed for emergency operating procedures and are developing "smart" procedures for the control room of the future. These procedures will be presented on color graphic screens and will be edited and/or updated frequently, based on the computer's knowledge of the actual state of the plant.

CANDU Personnel

Operator's Role. In the existing CANDU control rooms the separation of shift responsibility is divided among three individuals. The shift supervisor is in charge of the authorization of work and holds responsibility for power production. The work control area supervisor is responsible for scheduling, planning, and organizing work parties. The first operator is the senior power plant operator residing in the control room; he has always been thought of as a supervisor to some degree. The operator is considered to be the monitor of actions and has responsibility for the control actions performed. He can intervene and take over control of the situation whenever he so desires. However, the level of automation provided does not require any operator actions within 15 minutes of an unexpected or abnormal event.

The role of the operator has changed significantly from Pickering B to Darlington. In the Pickering B control room the operator is primarily responsible for observing and taking into account every single meter reading, whereas at Darlington the first operator assumes the role of a monitor. AECL believes that the first operator in the advanced control room will function in a "supervisory mode of control" and be both an operator and a maintainer. For control rooms of the future, the AECL staff is trying to develop tools that will let the human act as a thinker, planner, and supervisor.

Operator Demographics. The average age of CANDU control room operators is slowly increasing. The control room operating staff at the Darlington Generating Station will be a mixture of operators from Ontario Hydro's other nuclear facilities

and new employees. To become an auxiliary operator in one of Ontario Hydro's plants, an individual must have completed 13 years of schooling and two years of in-plant training. It takes about 8 to 10 years after that to be eligible for the position of first operator. Each of the four units at Darlington has one first operator on duty at all times.

Selection and Qualification Requirements. The increased use of digital equipment from earlier-generation plants to Darlington has not had an impact on selection and qualification requirements for control room operators. However, Darlington control room operators require some additional skills compared to Pickering B operators, notably a greater degree of computer literacy. AECL has indicated that, relative to the Darlington skills inventory, introduction of the advanced control room will have little, if any, impact on the selection and qualification requirements for control room operators. There are some who feel that for control rooms of the future, there may be no first operator. In this case, the shift supervisor effectively will be the first operator. As a result, the training, selection, and qualifications of this operator may change. However, the role of the operator is not expected to change drastically from what it is today.

CANADIAN POWER PLANT CONTROL ROOMS

CANDU Nuclear Power Plant Control Rooms

R.A. Olmstead (Olmstead 1992) has classified CANDU control rooms into the four classes given below with the features listed and the Canadian plants in which they are installed:

1. First Generation. Control rooms had fixed, discrete components (switches, lights, recorders, annunciators, etc.) arranged in an intuitive "common sense" way. Such systems were used in Canadian plants of the 1960s, and those still in use have been upgraded to include many features of the second generation control room.
2. Second Generation. Control rooms have video displays, keyboards, and information processing computers. Ergonomic and anthropometric standards (dealing with the size, shape, slope and other parameters of the physical interface in relation to the physical characteristics of the operators) have been applied to the physical layout of the control panels and the physical manipulation performed by the operators. Such systems are in use in the Pickering and Bruce plants today.
3. Third Generation. Control rooms place much more reliance on video display units as the primary source of information to the operators, while hardware

devices have been retained for the discrete logic drive controls. Display formats are more comprehensive and arranged in related hierarchical structures for ease of selection. Darlington is the first plant to have such a control room.

4. Fourth Generation. Control rooms utilize computer, electronic display and communication technologies of the 1990s, while human factors are used to address the cognitive aspects of operator performance. CANDU-3 will be the first Canadian plant of this class.

In the second generation control room, there is sufficient automation to ensure that no operator action is required in the first 15 minutes of any operational upset event. Automation is used to free the operators from tedious, distracting, stressful tasks to allow him/her to concentrate on more strategic matters. Examples include no requirement for operator action for a boiler feedwater transient after a reactor trip, and automatic warm-up and cool-down of the primary and secondary process systems.

In the third generation control room, more information is presented to the operators on video display units, allowing a reduction in the size of the overall control console. Considerable attention has been given to the anthropometric design of the panel. Hierarchical displays give both overview and detailed views of the systems in functional display formats developed specifically for Darlington. For instance, the display for the boiler swell/shrink situation contains all the data necessary to monitor the level and related setpoints at all power levels. The annunciator system has been enhanced to provide operators with more analytical capability after the initial flood of alarms.

In the fourth generation control room, many of the design requirements are based on theories established by the discipline of cognitive science to describe the behavior of humans as components in an information processing system. The human-machine interface design is driven by user requirements, and every effort is being made to elevate the role of the operator to that of system manager. Information is being packaged and presented in a context that is sensitive to the particular situation. Safety-critical parameters are continuously available for monitoring and control through a simple independent facility.

Features of Modern Canadian Power Plant Control Rooms

The first modern Canadian power plant control room console was developed for an oil-fired power plant at Courtenay Bay. It consists of four video displays and a single interactive keyboard. The CGDs are fully redundant and have been designed such that the plant can be controlled by only two of the video displays during any phase of operation. Except for the start-up phase, adequate control is possible from only one video display. Although the design of this console uses standards appropriate

to fossil plants, the experience gained has been invaluable in evaluating alternatives in the design of consoles for modern nuclear power plants.

The most modern Canadian power plant console currently in operation (since September 1991) is in the Ontario Hydro Lakeview coal-fired plant in Mississauga, Ontario. It is based on the Bailey INFI-90 distributed control system. The complete operator interface has five video displays, all fitted with touch screens for display and control selection. The interface is implemented on two proprietary "Management Command Systems," either of which is capable of full operation. The display and control information hierarchy is based on a combination of function- and system-oriented formats. Although the design is for a fossil plant, it is representative of the issues that can be addressed in design of advanced computer-based control rooms.

Each Darlington control room has a control panel approximately 34 feet long. Mounted across the top of this panel are a number of annunciation video displays, which are grouped by function. Three other video displays arranged across the middle of the panel are used to display system parameters and system drawings. Situated in front of the panel is a small console consisting of four video displays, where the first operator sits during the monitoring mode.

Computer-Generated Displays. The CANDU's CGDs are arranged in a hierarchical structure. CGDs in all CANDUs have been programmed so that they can be modified easily and quickly in order to present information in another manner or to add or delete specific parameters if the operators so desire. Alphanumerics are used in the system parameter CGDs, and the plant system CGDs utilize graphical symbology. The CGD screens present many types of data displays as well as symbols for valves, pumps, fans, dampers flow diagrams; bar graphs; and alarm messages. AECL's oil-fired power plant control room has three layers of cathode ray tube (CRT) screens. Alphanumerics and graphics are also used with these CGDs. The most recent alarm is displayed at the bottom of every screen. Screen functions are selected via a hierarchical system of menus. The screens can be adjusted and configured and the schematics can be edited on-line.

High-resolution color is presented on the video displays in all control rooms. However, because redundant information is presented by the symbology and the colors on the CGDs, the video displays can be run in monochrome if there should be problems with the color generators (or if the operator is "color blind"). Color coding is also used in the control rooms to depict the status of components and to help identify the severity of the plant status.

The main video displays in Ontario Hydro's control rooms support multiple users. They are totally redundant in that every CGD can be presented on all video displays.

Also, the operators can monitor any CGD on the four video displays on their control console. The control room can be operated by only one operator.

Controls. Ontario Hydro operators provide information to the control system through their control panels. Input includes start-up rate and the power levels to be maintained. In the fourth generation control room designed by AECL, operators are able to monitor the state of the plant and take control actions through the CGD console facilities. All control and data acquisition is accomplished via interactive graphics. The operators adjust automatic controller parameters and/or setpoints, acknowledge alarms, and perform data-logging activities via the video displays.

Expert Systems. The Canadian utility is developing a number of expert systems for its control rooms. One prototype is a knowledge based diagnostic system being installed in the Pickering Generating Station that will assist the operators in identifying the root cause of disturbances that have caused serious deviations in the plant's critical safety parameters. Both AECL and Ontario Hydro are developing several automated operator aids.

Organizational Support. Digital equipment appears to have been introduced into Ontario Hydro's control rooms in a manner that supports operator acceptance. Management wholeheartedly supports the use of advanced I&C in its nuclear generating station control rooms. Also, operators were involved in the design process starting early in the development process. They were also thoroughly trained on the digital I&C before it was implemented. Training on the digital I&C in the simulator has had much to do with operator acceptance of advanced technology.

Changes in the control rooms have been well accepted by operating personnel at Ontario Hydro, and the operators are enthusiastic about the modifications. Their early involvement in control room design gave designers prompt feedback on the operator interface and promoted early understanding of the system by the operators.

Control Room for New CANDU Stations

AECL is designing its advanced "fourth generation" control rooms for the CANDU-3 and CANDU-9 using a computer-aided design system. Each control room will consist of a control panel and two consoles: a main control console and a safety system testing console. The panel will include areas for the shutdown systems, emergency core cooling, primary heat transport, reactor regulating system, digital control computers, boiler control, feedwater systems, condenser and turbine, and support services. Each panel will have three physical levels: at the top will be the annunciation system windows; in the middle will be the video displays and monitoring instruments; and at the lowest level will be switches, controls, and keyboards. The main control console will allow access to all of the computer setpoints and displays which are available at the video displays mounted in the

control panel. The control room will also have large, dynamic color mural mimics depicting the major equipment and system status of the entire plant.

Ontario Hydro and AECL are working on a number of automated operator aids for alarm analysis, heavy water inventory, plant analysis, status monitoring, diagnostic monitoring, secondary heat transport, process control, fault diagnosis, spent fuel bundle count, and development of training manuals. The operator aids are being evaluated and used in the simulator before they are implemented in the control room. Ontario Hydro and AECL are members of a CANDU Owners Group (COG) that is determining where the Canadian industry should be going in regard to on-line operator aids.

AECL is also developing the control room of the future (10 to 15 years from now). It will be a compact module and will contain a few sit-down consoles that will provide the operators with information that has been processed to reflect the context of their specific objectives and tasks in each particular situation. Current plant status at the most detailed level will be available on CCD screens in the form of computerized flowcharts.

Operator's Companion

An indication of future developments in advanced CANDU control room operations is the "Operator Companion," a series of concepts being considered for future control rooms that would inform and advise the operator on all aspects of plant operation in a manner that is not possible with conventional I&C systems. Some of the features of these concepts include:

1. Context-sensitive information displays to provide the operator with information that has been processed to reflect the context of his/her specific objectives and tasks in each particular situation,
2. Detailed operating instructions, edited to reflect the actual state of the plant, to be presented using color graphic screens, voice annunciation and automatic confirmation of essential prerequisites to action,
3. Several expert systems for a variety of specific tasks, especially those that are not routine, to assist the operator,
4. A large dynamic color graphic mural mimic depicting the major equipment and system status of the entire plant to provide the operator with a mental model of the plant,
5. Control room displays designed to exploit cognitive science by presenting alarm configurations and plant parameter deviations in the form of interpretable patterns,

6. An operator decision support system to provide the operator with root cause diagnostic information during any type of operation, including the answers to "what if?" questions and the rationale for any recommendations, and
7. An operation information system to electronically integrate and automate "routine" activities associated with the operation of a plant (i.e., maintenance records, work control, equipment status, event logging, schedules, etc.).

CANDU-3 DIGITAL I&C AND SAFETY SYSTEMS

As an indication of the state-of-the-art in digital instrumentation and control systems and safety systems, the new CANDU-3 design is described here in considerable detail. The CANDU-3 design promises substantial safety and operational benefits, as well as cost reductions, by taking advantage of the rapid evolution of digital technology and human factors engineering. The following are some of the most significant features and benefits:

1. Many fixed indicators and controls have been eliminated and replaced by interactive video stations and large mural mimics that display and communicate overall plant status and support group decision making.
2. Trunk cabling, relays, timers, comparators, etc. have been replaced with distributed control processors to provide a substantial reduction in complexity.
3. Repetitive, error-prone tasks such as periodic testing are being automated.
4. The emergency response facility is an extension of the comprehensive information management facility available in the CANDU control room.
5. The control room interactive video displays include procedure-driven displays to support the tasks required for operation.
6. A critical annunciation system will provide operators with a short list of priority alarms related to predetermined critical safety parameters and emergency operating procedures during major plant disturbances.

Plant Display System

In the CANDU plant display system (PDS), two computers collect most of the plant data through a pre-processing computer from the distributed control system (DCS). The balance of data, that associated with the special safety systems, is obtained from the field through a similar set of database computers called the safety system monitor (SSM). The PDS database computers transmit plant information to redundant local area networks (LANs) which supply information to five operator

workstations (each with three video displays, a keyboard and a graphics position device) to produce the display and supervisory control interface between the plant and the operator. Similarly, information from the SSM can be routed to two operator workstations, one in the main control area and one in the secondary control area.

The hardware and software are open in architecture and adhere to computer industry standards so that they can be expanded, if desirable at a later date. Each of the nodes on the network are industrially hardened, general-purpose computers drawn from a family of computer products connected through a commercial LAN. The system is designed such that the whole system can function in a closely coupled fashion much like a multiprocessor computer.

Widely-used commercial, off-the-shelf software components are used for the PDS. At the present time, POSIX (Portable Operating System Interface) standards for the operating system are being used. An industry standard windowing environment, such as X-Windows (standard windowing software for workstation and large computer environments) and Open Look or Motif (both are window manager software packages that give the "look and feel" to the windowing environment) are being used. The software is being developed in one or more of the ANSI standard programming languages (such as C or C++).

Distributed Control System

Data acquisition and process control functions for non-safety systems are performed by an advanced distributed digital control system. This includes change-of-state detection and time stamping for selected binary events. It controls low-level and interlocking functions for individual process devices (such as pumps, valves, solenoids, etc.), as well as high level control and coordination functions for groups of devices and systems (steam generator level control, system pressure and inventory control, etc.). The scope includes manual and automatic mode changes, setpoint changes, and control actions carried out in response to operator commands.

The DCS consists of a number of signal scanning and processing stations linked by high performance data highways. An optimal compromise between geographic and functional partitioning has reduced the complexity of the cabling and wiring. The system is divided into three separate channels to match the channelization of redundant sensors and process devices. Each channel has redundancy, self-checking and automatic switchover concepts to provide a fault tolerant system. The data links are redundant and buffered to avoid compromising system reliability.

Digital Protection Systems

The digital protection systems (DPSs) of the CANDU-3 are evolutionary versions of those in the Darlington plant, and the performance is expected to be as good or better than that achieved with the earlier plants. Such performance is due largely

to the design that employs features such as self-checks, "continuous" checking hardware watch-dog timers, etc., which convert detected unsafe failures into safe failures (i.e., trip the channel).

Assurance of Adequate Software Quality

In licensing the CANDU-3, the problems raised by the Canadian AECB will have to be addressed. This time the solution will be integrated into the design and development process. The steps taken include the following:

1. Establish guidelines for categorizing software according to the nuclear safety impact of a potential failure and the safety related reliance placed on the system of which the software is a part.
2. Prepare software standards and tools for the complete development life cycle of safety system software, including software maintenance.
3. Establish requirements for safety-critical system software, which is to be restricted to an absolute minimum and segregated from non-critical software.
4. Prepare unambiguous specifications in the early design phases that can be analyzed to ensure that requirements are correct, consistent and complete. This minimizes the transmission of conceptual errors into the detailed design stages and facilitates verification of the software against the specifications.
5. Produce software according to modern software engineering techniques and a set of established CANDU software design principles to achieve a fail-safe and robust design. This assures well-structured design with cohesive software modules and clearly defined minimal coupling between those modules. Diverse software and hardware are being used, where appropriate, to minimize common mode errors.
6. Subject the completed software product to multiple levels of systematic verification and testing. Normal software testing of units, integration, and systems are performed using automatic tools where possible, and each stage in the development process is systematically verified against the previous stage.

SAFETY IMPLICATIONS OF CANDU EXPERIENCE WITH DIGITAL SYSTEMS

The clear superiority of digital systems as demonstrated by the CANDU experience, with their ability to diagnose impending failures and initiate a fail-safe action, is a significant safety issue that should be of special interest to every utility. The increased safety of digital over analog systems is a critically important point. This

undoubtedly will become an even more definitive advantage with the aging of analog hardwired safety systems common in most U.S. plants. Periodic testing initiated by humans is the accepted method of detecting failures in analog hardwired components, but this type of testing is subject to human error. Reallocation of the test function to a computer clearly improves safety. Pertinent questions are as follows:

1. Are faults in analog hardwired systems being detected in a timely manner? (The test must be much shorter than failure period to detect failures in a timely manner.)
2. Does aging of this equipment require shorter test periods to detect faults in a timely manner?
3. How significant are the human errors associated with testing? Are data available on the error rate?
4. Are the test performance indicators in current use sufficiently sensitive to detect performance differences between analog and digital safety system components?

The potential safety implications of the advanced I&C systems identified above, as well as the adequacy of current NRC guidelines to deal with these systems, are issues that will need to be addressed by the regulatory authorities as advanced systems are introduced into nuclear power plants.

REFERENCES

- Carter, R.J. and R. E. Uhrig, *Human Factors Issues Associated with Advanced Instrumentation and Controls Technologies in Nuclear Plants*, NUREG/CR-5439, ORNL/TM-11319, Oak Ridge National Laboratory, Oak Ridge, TN, June 1990.
- Fenton, E. F., K. M. Iwasa-Madge, and R. A. Olmstead, *Fundamental Objectives and Emerging Trends in CANDU Control Center Design*, COG Computer Conference, Markham, Ontario, 1990.
- Ichiyen, N. (AECL CANDU) and P. Joannou (Ontario Hydro), "The Canadian Approach to Digital Systems in CANDU Safety Systems," *Nuclear Engineering International*, Sept. 1991.
- Lepp, R. M., and L. M. Watkins, *Control and Instrumentation Systems for the 600 MWe CANDU PHW Nuclear Power Plants*, AECL-7519, Atomic Energy of Canada Limited, Chalk River, Ontario, 1982.

- Lipsett, J. J., R. A. Olmstead and J. E. S. Stevens, *Balancing the Roles of Humans and Machines in Power Plant Control*, AECL-9955, IAEA Advisory Group Meeting on the Balance Between Automation and Human Actions, Vienna, Austria, April 17-21, 1989.
- Lupton, L. R., J. J. Lipsett, R. A. Olmstead, and E. C. Daver, "A Foundation for Allocating Control Functions to Humans and Machines in Future CANDU Nuclear Power Plants," *IAEA International Symposium on Balancing Automation and Human Action in Nuclear Power Plants*, Munich, FRG, July 9-13, 1990.
- Lupton, L. R., E. C. Davey, P.A. Lapointe and R. R. Shah, "Integrated Control Centre Concepts for CANDU Power Plants," AECL-10110, *ANS Topical Meeting on Advances in Human Factors Research on Man-Computer Interactions: Nuclear and Beyond*, Nashville, TN, June 10-14, 1990.
- Lupton, L. R., L. L. Anderson and R. A. J. Basso, "The AECL Operator Companion--An Overview," AECL-10074, *International Symposium for Demonstration of Expert Systems Applications to the Power Industry*, Montreal, Quebec, May 7-12, 1989.
- National Research Council, *Human Factors Research and Nuclear Safety*. Washington, D.C.: National Academy Press, 1988.
- Norman, D. A., "Some Observations on Mental Models." In D. Gentner and A. L. Stevens (Eds.), *Mental Models* (pp. 7-14). Hillsdale, N.J.: Lawrence Erlbaum Associates, 1983.
- Olmstead, R. A., "The CANDU-3, Innovative Application of Digital Technology," *EPRI Conference on Advanced Digital Computers, Controls and Automation Technologies for Power Plants*, San Diego, California, February 5-7, 1992.
- Pauksens, J., A. Condor, J. R. Popovic and A. Rosever, "Canadian Experience with Computerized Scram," *Third International Meeting on Nuclear Power Plant Thermal Hydraulics and Operation*, Seoul, Korea, November 1988.
- Popovic, J. R., and G. J. Hinton, "CANDU Computerized Safety System," *IAEA International Workshop on the Safety of Nuclear Installations of the Next Generation and Beyond*, Chicago, IL, August 28-31, 1989.
- Pulliam, R., H. E. Price, J. Bongarra, C. R. Sawyer, and R. A. Kisner, *A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control* (NUREG/CR-3331). Washington, D.C.: U.S. Nuclear Regulatory Commission, 1983.

- Rasmussen, J., *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*. New York, N.Y.: North-Holland, 1986.
- Shneiderman, B., *Designing the User Interface: Strategies for Effective Human-Computer Interface*. Reading, Mass.: Addison-Wesley Publishing Company, 1987.
- Smith, S. L., and J. N. Mosier (1984). *Design Guidelines for the User Interface for Computer-Based Information Systems*. Bedford, Mass.: The Mitre Corporation, 1984.
- Uhrig, R. E., and R. J. Carter, *Survey of Canadian Uses of Digital Computers in Control, Safety Systems, and Human-Machine Interfaces in Nuclear Power Plants*, ORNL/NRC/LTR-89/6. Oak Ridge National Laboratory, 1989.
- Uhrig, R. E., and R. J. Carter, *Program Plan for Regulatory Research on Expert Systems*, ORNL/NRC/LTR-89/5. Oak Ridge National Laboratory, 1989.
- U.S. Nuclear Regulatory Commission, *Guidelines for Control Room Design Reviews*, (NUREG-0700), Washington, DC, 1981.

JTEC/WTEC reports are available from the NTIS, 5285 Port Royal Road, Springfield, VA 22161 (703) 487-4650. Prices are as of 12/92 and subject to change. Add postage plus \$3.00 for handling per order, not per report. Add \$7.50 for billing if order is not prepaid. These prices are for the U.S., Canada and Mexico. Information via Fax: (703) 321-8547.

JTECH Panel Report on Computer Science in Japan
(12/84) PB85-216760
E06/E01 (\$25.50/12.50)*

JTECH Panel Report on Opto and Microelectronics
(5/85) PB85-242402
E10/E01 (\$38.00/12.50)

JTECH Panel Report on Mechatronics
in Japan (6/85) PB85-249019
E04/E01 (\$20.50/12.50)

JTECH Panel Report on Biotechnology
in Japan (5/86) PB85-249241
E07/E01 (\$28.50/12.50)

JTECH Panel Report on Telecommunications
Technology in Japan (5/86) PB86-202330/XAB
E08/E01 (\$32.00/12.50)

JTECH Panel Report on Advanced Materials (5/86)
PB86-229929/XAB
E08/E01 (\$32.00/12.50)

JTECH Panel Report on Advanced Computing in
Japan (12/87) PB88-153572/XAB
E04/A01 (\$20.50/9.00)

JTECH Panel Report on CIM and CAD for
the Semiconductor Industry in Japan (12/88)
PB89-138259/XAB
E07/A01 (\$28.50/9.00)

JTECH Panel Report on the Japanese Exploratory
Research for Advanced Technology (ERATO)
Program (12/88) PB89-133946/XAB
E09/A01 (\$35.00/9.00)

JTECH Panel Report on Advanced Sensors in Japan
(1/89) PB89-158760/XAB
E11/A01 (\$41.00/9.00)

JTEC Panel Report on High Temperature
Superconductivity in Japan (11/89)
PB90-123126
E10/A02 (\$38.00/12.50)

JTEC Panel Report on Space Propulsion in Japan
(8/90) PB90-215732
E10/A02 (\$38.00/12.50)

JTEC Panel Report on Nuclear Power in Japan
(10/90) PB90-215724
A14/A02 (\$52.00/12.50)

JTEC Panel Report on Advanced Computing in Japan
(10/90) PB90-215765
A10/A02 (\$36.50/12.50)

JTEC Panel Report on Space Robotics in Japan (1/91)
PB91-100040
E14/E01 (\$52.00/12.50)

JTEC Panel Report on High Definition Systems in
Japan (2/91) PB91-100032
E14/E01 (\$52.00/12.50)

JTEC Panel Report on Advanced Composites in Japan
(3/91) PB90-215740
E10/E01 (\$38.00/12.50)

JTEC Panel Report on Construction Technologies in
Japan (6/91) PB91-100057
E14/E01 (\$52.00/12.50)

JTEC Program Summary (9/91)
PB92-119429/XAB
E10/E01 (\$38.00/12.50)

JTEC Panel Report on X-Ray Lithography in Japan
(10/91) PB92-100205
E10/E01 (\$38.00/12.50)

WTEC Panel Report on European Nuclear
Instrumentation and Controls (12/91)
PB92-100197
E14/E04 (\$52.00/20.50)

JTEC Panel Report on Machine Translation in Japan
(1/92) PB92-100239
E10/E02 (\$38.00/15.50)

JTEC Panel Report on Database Use and Technology
in Japan (4/92) PB92-100221
E10/E02 (\$38.00/15.50)

JTEC Panel Report on Bioprocess Engineering in
Japan (5/92) PB92-100213
E14/E04 (\$52.00/20.50)

JTEC Panel Report on Display Technologies in Japan
(6/92) PB92-100247
E14/E04 (\$52.00/20.50)

JTEC Panel Report on Material Handling
Technologies in Japan (2/93) PB93-128197

JTEC Panel Report on Separation Technology in
Japan (3/93) PB93-159564

JTEC Panel Report on Knowledge-Based Systems in
Japan (5/93) PB93-170124

NASA/NSF Panel Report on Satellite Communications
Systems and Technology (7/93) PB93-209815

WTEC Monograph on Instrumentation, Control and
Safety Systems of Canadian Nuclear Facilities (7/93)
PB93-218295

*First code & price are for hardcopy; the second for microfiche.

ISBN 1-883712-24-6