Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

CMD 19-M43

Date: 2019-10-28
File / dossier : 6.02.04
Edocs pdf : 6030605

Update from CNSC Staff

Mise à jour du personnel de la CCSN

Status of Digital Control Computer Systems

État des systèmes informatiques à commande numérique

Action item from May 15, 2019 Commission Meeting (#19298)

Mesure de suivi de la réunion de la Commission du 15 mai 2019 (#19298)

Commission Meeting

Réunion de la Commission

November 6, 2019

Le 6 novembre 2019

Canada

This page was intentionally left blank

Cette page a été intentionnellement laissée en blanc

Canadian Nuclear Safety Commission   Commission canadienne de sûreté nucléaire

MEMORANDUM - NOTE DE SERVICE

Security Classification/Classification de sécurité	**UNCLASSIFIED**
Our File – Notre référence	e-DOC # 6028934
Your File – Votre référence	
Date	2019-10-28
Tel. No. – N° de tél.	613-995-2655

To
A
M. Leblanc
Secretariat

From
De
G. Frappier
Director General
Directorate of Power Reactor Regulation

Subject
Objet
Closure of Commission Action #19298, Status of Digital Control Computer (DCC) Systems

Purpose

The Commission requested CNSC staff, under RIB action #19298 [1], to provide information about the aging management of Digital Control Computer (DCC) across Canadian nuclear reactors, and how it is managed across Canada's nuclear reactor fleet [2]. The purpose of this memorandum is to disposition the Commission action by providing a brief background, description, and the status of DCC systems. In particular, this memorandum describes how the aging of DCC systems is managed to ensure the continued safe operation of Canadian Nuclear Power Plants (NPPs).

Background

CANDU plants have been pioneers in the use of computer-based control systems for NPPs. DCC systems have been used in all commercial CANDU NPPs built, starting with Pickering A. The IBM 1800 computers were used in Pickering A units. Computers based on the VARIAN V7x series architecture have been used in all other CANDU NPPs, except Darlington, which uses DCCs based on DEC PDP-11/70 computers. Although some design and implementation details differ between stations, all DCCs operating in Canadian NPPs have similar hardware and software architectures, as well as basic system functionalities and behaviour.

DCC systems play an important role in the safe and reliable operation of CANDU NPPs as they are used to monitor and control major reactor power and electrical power generation functions. In Normal Operation (NO) conditions, these control functions are used to maintain the plant within acceptable control performance limits. During abnormal conditions, some functions are designed to respond with the goal of avoiding the need for Shut-Down System (SDS) action (manual or automatic); keeping all essential reactor and plant parameters within specified limits. It should be noted that one of the CANDU fundamental design principles is the separation of control and protection functions. This principle ensures that the failure of DCC systems will not compromise functions of the shutdown systems.

Each CANDU unit is controlled and monitored by a DCC system which consists of two identical, independent computers, DCCX and DCCY (or DCC1 and DCC2 at Pickering A). Functions that are essential to the safe operation of the unit are incorporated into both computers. Although both DCCs provide their own separate sets of control signals, relay interlocks ensure that only the master DCC output signals are connected to system field devices.

Within each computer, the software and hardware operations are continuously monitored by a combination of internal software and hardware self-checking systems and independent Watchdog Timers (WDTs). A fault in any essential part of the master computer results in automatic transfer of control to the standby computer. A DCC system is organized so that maintenance on the standby computer can take place while the unit is being controlled by the other computer. In addition, the DCC system is modular, allowing components and subcomponents of the DCC system to be replaced during maintenance processes.

All critical inputs to a DCC are duplicated or triplicated. Input signals are checked by control programs to ensure that they are valid for use. If a control function on one DCC does not have sufficient valid inputs to proceed, the control function will be removed from service. Subsequently, the same control function on the other DCC will takeover the control via the failover mechanism. This function-by-function control transfer mechanism eliminates the potential for unintended DCC control actions being taken as a result of a single faulty input.

In the event that both computers fail (dual stall), the unit will automatically or manually shutdown. The power decrease is initiated through the actions of WDTs, which ensure that all computer outputs are isolated from the plant, and are forced to a fail-safe condition. This will result in the decrease of reactor power by the dropping of control absorbers and/or liquid zone control compartment flooding.

DCC dual stall is an initiating event and is analyzed in both Deterministic and Probabilistic Safety Analysis (PSA) reports, and is also reported and tracked in the Annual Reliability Report (ARR).

Since DCC failures may cause unplanned reactor power changes, this is reportable under CNSC REGDOC-3.1.1 Reporting Requirements for Nuclear Power Plants [3], which is another level of oversight on DCC performance.

The DCC system hardware is composed of the following five subsystems: *i)* computer; *ii)* input/output subsystem; *iii)* interfaces and peripherals; *iv)* power supplies and fans; and *v)* inter-process communication and transfer of control. DCC aging management covers these aforementioned subsystems.

In addition, the DCC system is connected to field devices (inputs) to obtain real-time information from the plant and send commands to field devices (outputs) for control. Aging management of these field devices and associated power supplies is covered by their corresponding component/ system specific aging management plans.

Aging Management of Digital Control Computer Systems

General

Over the past forty years, DCCs and their associated software have demonstrated the reliability required for CANDU NPP operations. Licensees' aging management strategies have played an important role in ensuring the reliable and safe operation of computer-based control systems.

All licensees have aging management related activities for DCC systems within existing design, operation and maintenance programs, for example:

- Preventive maintenance activities to ensure DCCs meet their reliability target(s);
- Inspection programs for evaluating the effectiveness of maintenance plans, monitoring the procurement and operation of qualified spare parts, and ensuring the reliable operation of the DCCs to the end of plant life;
- System health monitoring programs for assessing DCC component degradation, including aging related degradations and depletion of qualified spare parts. Modification and replacement of obsolete/degraded equipment are planned and documented in DCC health report;
- Training programs to ensure that the requisite DCC maintenance and engineering capabilities are maintained to support the technology;
- Procurement programs to ensure there are adequate qualified components available;
- Periodic safety reviews for a more comprehensive assessment of DCC aging effects and actions delineated in the Integrated Implementation Plan (IIP);
- Plant life management programs to proactively find solutions for the whole DCC life cycle, including plant life extension. This includes engineering replacement of obsoleted DCC subsystems, as further illustrated below.

All licensees continue to make improvements and upgrades to their DCC systems in accordance with their maintenance plans.

Based on the information collected in the CNSC compliance verification activities, staff can confirm that all licensees implemented processes and programs to address aging and obsolescence of DCC systems. All Canadian NPP sites meet the applicable requirements and safety expectations set forth in CNSC's REGDOC 2.6.3 Fitness for Service: Aging Management [3].

Main Challenges for the Replacement DCCs:

In a broad sense, a DCC system is composed of two parts: the hardware and the software. DCC hardware is essentially electronic Instrumentation and Control (I&C) equipment. Physical aging of electronic I&C equipment includes:

- Aging mechanisms;
- Effects of aging;
- Reliability estimation;
- Failure modes due to aging; and
- Mitigating measures.

These are well understood by the nuclear industry [5, 6, 9, 10, 11, 12]. All licensees follow the guidelines and recommendations from industrial reports and standards for managing aging of DCC systems [7, 8, 10, 11, 12, 13, 14].

The aging management strategy for DCC systems has evolved from the early 1990s, when Original Equipment Manufacturers (OEMs) stopped supporting these computers and qualified spare parts became difficult to find. In the early 1990s, Pickering A forecasted that acquiring spare parts and repairing defective parts alone would not be sufficient to sustain the reliable operation of their DCCs to support long-term operation of the plant. The industry foresaw that these DCCs would need to be replaced [15].

DCC system functions are implemented by software. This software has been extensively validated and improved during many decades of plant operation, but there are no qualified tools to port DCC software to a different hardware environment. Therefore, a fundamental element of DCC aging management has been retention of the time-proven DCC software [10, 15, 17].

The approach selected by OPG for the replacement of the DCCs was to procure and qualify a hardware emulator with sufficient fidelity (function and performance). This hardware would specifically emulate the IBM 1800 hardware, such that the existing Pickering A DCC application software could run on the new hardware platform without modification.

Extensive supplementary testing was performed by OPG personnel to qualify the emulator. A project was undertaken to replace the IBM 1800 DCCs with the newly qualified ES-1800. The ES-1800 used more modern technology than the IBM 1800, and consequently spare parts could be easily obtained [15].

ES-1800 computers were successfully installed on Units 1 and 4 at Pickering A. Post replacement, the Pickering A DCCs have run without any emulator attributable faults and their system health indicator has improved dramatically [15].

Subsequent to the Pickering A replacement, replacing obsolete computers with a hardware emulator is common practice in nuclear and other safety critical industries to ensure the integrity (no modification) of existing application software. For example, the ES 1800 hardware emulator selected by OPG was developed to replace the IBM 1800 computers used by the United States military [15]. Another example [17] is from Électricité de France (EDF) where it used hardware emulators to manage the obsolescence of the Motorola MC68000 microprocessor based controllers used in various control systems in its 1,300MW series NPPs.

Research and Development for the Replacement of DCCs

Research and development has played an important role in the aging management of DCCs. All licensees, including international CANDU owners, have participated in a CANDU Owner's Group (COG) project (COG joint project 4048) to examine the maintenance, reliability and upgrade history of all Canadian CANDU plants that use the Varian-based DCCs. The charter of this project was to identify any specific cost-effective incremental upgrades, design enhancements, or maintenance procedures. A set of twenty-four criteria was applied, including risk due to system design change, risk due to software changes, risk due to project complexity, etc. The four utilities (Bruce Power, Hydro Quebec, NB Power, and OPG) applied the criteria and the hardware emulator approach was the unanimous choice.

On behalf of all licensees, including international CANDU owners, COG purchased the Intellectual property (IP) rights to remanufacture Varian 7x hardware emulators (SSCI-890). These emulators will be used to replace Varian 7x based DCCs for all project member utilities. COG has also secured technical support for CANDU DCCs until at least year 2035.

Station Status of Aging Management of Digital Control Computer System

Bruce (Unit 1 – 8):

Bruce Unit 1 – 8 DCC systems use Varian 72 computers commissioned during 1970s and 1980s. Bruce has completed numerous DCC related improvements/upgrades.

Bruce Power reported that there are adequate spare parts to support the end of life of the plant. In order to support life extension of both plants, Bruce Power is planning to replace the DCCs. The selected platform for the DCC replacement is SSCI-890 systems which have been successfully used to replace DCCs in Point Lepreau and the Embalse CANDU plant in Argentina. The target date for installation on Unit 6 is 2022. The project progress is being monitored by CNSC staff via IIP actions.

Darlington (Unit 1 - 4):

At Darlington, the original DCC computers (PDP 11/70) were replaced in the 2000s by newly qualified computer hardware emulators (QED-970) [18] using current technology. The manufacturer of this computer hardware emulator still provides support for this product.

During the Darlington refurbishment, some DCC subsystem components will be replaced. These replacements are being monitored by CNSC staff via IIP actions.

Pickering A (Unit 1 and 4):

At Pickering A, the original DCC computer (IBM 1800) of Unit 1 and 4 were replaced with newly manufactured computer (ES-1800) in 2002. OPG has acquired an adequate number of spare parts to sustain Unit 1 and 4 DCCs until the end of commercial operation.

OPG reported recently that the Pickering Unit 1 and 4 DCC systems are expected to support the plant to beyond end of commercial operations. To maintain current operations and support beyond end of commercial operations, a number of projects are underway or were completed to replace some DCC subsystem components.

Pickering B (Unit 5 - 8):

Pickering B Unit 5 – 8 DCC systems are based on VARIAN 72 computers. Pickering B has completed numerous DCC related improvements/upgrades.

OPG reported recently that the Pickering B Unit 5 – 8 DCC systems are expected to support the plant to beyond end of commercial operations. To maintain current operations and support beyond end of commercial operations, a number of projects are underway or were completed to replace some DCC subsystem components.

Point Lepreau:

At Point Lepreau the original DCC computer (Varian 73) was replaced with newly manufactured equipment (SSCI-890) under a DCC life extension program progressed during and after the refurbishment outage.

The progress of this program was tracked by the CNSC under Action Item 071220. This Action Item was closed in 2016.

In partnership with other utilities via the CANDU Owners' Group, NB Power maintains a renewable long-term support agreement with the equipment manufacturer intended to facilitate operation of the DCCs for the remainder of the plant's life.

CNSC Oversight of Digital Control Computer System Aging Management

CNSC staff conduct regulatory oversight of DCC aging management through various compliance verification activities. These activities include:

- Identifying potential negative trends of digital control computer systems through site staff routine surveillance activity; attending Plant Health Committee meeting; reviewing system health reports and relevant event reports;
- Periodically monitoring actual conditions of digital control computer system by reviewing periodic safety reports;
- Monitoring the execution of DCC aging management plans by reviewing condition assessment or evaluation reports;
- Reviewing replacement project management plans of major DCC components, such as replacement of the computers;
- Type II inspections such as software maintenance and electrical power systems inspection for Class I and Class II power systems used by DCC systems.

CNSC staff:

- Have reviewed DCC replacement plans for Pickering A, Darlington, Point Lepreau, and Gentillly-2;
- Are currently monitoring the progress of Bruce A/B digital control computer modernization project;
- Are planning to conduct a Type II aging management inspection of the Pickering site and the DCC was selected as one of the systems that will be inspected.

Conclusion

The industry has an active program to manage aging of the DCC. Through compliance oversight CNSC staff ensure that DCC aging is being managed adequately according to applicable regulatory requirements and safety expectations.

References:

Regulatory Requirements:

[1] CNSC RIB #19298 DPRR: Digital Control Computers (DCC) Aging Management, https://rib-bir.cnsc-ccsn.gc.ca/ActionModule/ActionView.aspx?id=19298

[2] CNSC Minutes of Canadian Nuclear Safety Commission (CNSC) Meeting Hold on May 15, 2019, E-DOCS-#5910107

[3] CNSC REGDOC 2.6.3 Rev. 1.0, Fitness for Service: Aging Management, March 2014.

[4] CNSC REGDOC 3.1.1 Rev. 1.0, Reporting Requirements: Reporting Requirements for Nuclear Power Plants, March 2014.

General References:

[5] DOD Standard, MIL-HDBK-217, Reliability Prediction of Electronic Equipment, March 14, 1997.

[6] EPRI TR/1003568, Collected Field Data on Electronic Part Failures and Aging in Nuclear Power Plant I&C Electrical Boards and Systems, 2002.

[7] EPRI TR/1007916, Printed Circuit Board Maintenance, Repair, and Testing Guide, October 2003.

[8] EPRI TR/1008166, Guidelines for the Monitoring of Aging of I&C Electronic Components, October 2004.

[9] EPRI TR/1011709, Evaluating the Effects of Aging on Electronic Instrument and Control Circuit Boards and Components in Nuclear Power Plants, May 2005.

[10] IAEA, TECDOC-1147, Management of Ageing of I&C Equipment in Nuclear Power Plants, June 2000.

[11] IAEA TECDOC-1402, Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance, August 2004.

[12] IAEA TECDOC 1503, Nuclear Power Plant Life Management Processes: Guidelines and Practices for Heavy Water Reactors, July 2006.

[13] IEC 62342, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Management of Ageing, August 2007.

[14] IEEE Std. 1205, IEEE Guide for Assessing, Monitoring, and Mitigating Aging Effects on Electrical Equipment Used in Nuclear Power Generating Stations and Other Nuclear Facilities, 2014.

[15] Rick Hohendorf, Nuclear Power Plant Control Computer Aging Management Strategy, Implementation and Results, IAEA Technical Meeting on Integrating Analog and Digital I&C Systems in Hybrid Main Control Rooms at NPPs, 2007.

[16] IBM 1800, https://ethw.org/IBM_1800.

[17] Book, Zhijian Zhang, Hidekazu Yoshikawa, Progress of Nuclear Safety for Symbiosis and Sustainability: Advanced Digital Instrumentation, Control and Information Systems for Nuclear Power Plants, March 2014.

[18] EPRI Report TR/1019181, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems, December 2009.