SLOWPOKE INTEGRATED REACTOR CONTROL AND INSTRUMENTATION SYSTEM (SIRCIS)

Lt(N) L. R. Cosby
Department of Chemistry and Chemical Engineering • Royal Military College of Canada
PO Box 17000 Stn Forces • Kingston, Ontario, Canada • K7K 7B4
cosby-l@rmc.ca

I. ABSTRACT

A Commercial Off-The-Shelf (COTS) digital control and instrumentation system was developed for the SLOWPOKE-2 reactor at RMC using the LabVIEW Professional Development System. The resulting software was deployed on a PowerMac G4 computer using Mac OS 9.1. Several techniques were used to enhance the robustness of this COTS system.

II. INTRODUCTION

SLOWPOKE is a small, inherently safe, pool-type research reactor that was engineered and marketed by Atomic Energy of Canada Limited (AECL) in the 1970s and 80s. The original reactor, SLOWPOKE-1, was moved from Chalk River to the University of Toronto in 1970 and was operated until upgraded to the SLOWPOKE-2 reactor in 1973. In all, eight reactors were produced and six are still in operation today, two having been decommissioned. All of the remaining reactors are designated as SLOWPOKE-2 reactors.

In total, three variations of control systems were used for SLOWPOKE reactors:

- the original control system for SLOWPOKE-1;
- the Mark 1 (MK1) control system, installed at the University of Toronto, Dalhousie University (Dal), École Polytechnique (EP), the University of Alberta (U of A); and
- the MK2 control system (Figure 1), installed at the University of the West Indies (UWI), Saskatchewan Research Council (SRC), and the Royal Military College of Canada (RMC).

The SLOWPOKE-2 research reactor at RMC was commissioned in 1985 with the MK2 control console, which includes auxiliary equipment located in a rack mount cabinet. Although it is called a controller, it has several functions, which include conditioning of transducer signals, monitoring and display of measured parameters, and closed feedback control of a single control rod.

Figure 1 - SLOWPOKE-2 Control System at RMC

The system performs both control and instrumentation roles.

The reactor is currently in its 16th year of operation, which may be considered to be approximately mid-life for the reactor. The reactor as a whole has operated reliably, as have the other SLOWPOKE reactors, partly due to the simplicity of the reactor. There is only one moving part and that is the cadmium control rod, which is suspended inside the core by a wire attached to the control motor.

The weakest link with SLOWPOKE reactors is the control system, which has reliability, availability and maintainability issues. Essentially, as the system ages, parts fail more frequently and the system becomes increasingly more difficult to maintain. Based on these facts, an investigation was conducted to determine the feasibility of implementing a new control system for the reactor. The result of this effort is known as the SLOWPOKE Integrated Reactor Control and Instrumentation System (SIRCIS).

A commercial control system or some variant thereof was entertained for some time. However, the cost of a commercial system was determined to be likely in excess of $500k for a turnkey solution. An expenditure of this level would not have been easily justified in view of the annual income that the SLOWPOKE-2 Facility can dependably generate. It must be understood that universities in general cannot easily afford large capital projects of this nature without significant commercial return. For these reasons, it was decided to approach the development of a new control system with COTS components. The intent with SIRCIS was to transfer the main functionality from the MK2 control system, while improving on functionality and interaction where practical and desired. Also, it was necessary to upgrade the system to reflect additions to the Facility, e.g., the Neutron Beam Tube (NBT), as well as improve safety-related functions.

An analog system was never seriously considered for this upgrade since the advantages of digital control were quite clear from the outset:

- most new or replacement control and instrumentation systems for reactors today are software-based digital systems (e.g., MAPLE, NRU, Penn State Breazeale, Darlington CANDU);
- analog systems are not easily reconfigurable once built, whereas digital systems can be readily modified;
- software-based solutions are more suitable to rapid prototyping methods, thus reducing development time and cost considerably;
- software-based control systems have fewer failures once the code is debugged; and
- digital systems generally enjoy reduced maintenance costs.

Once it became evident that a digital software-based system was the best general option to pursue, development options were considered. All options were based on Commercial-Off-The-Shelf components and technology.

III. COTS

The cornerstone of using a COTS approach in a control and instrumentation application lies in using commercially available components, both hardware and software. The reason that COTS has garnered such support in recent years is

that there are several distinct advantages to applying COTS principles:

- lower cost hardware and software;
- lower development cost;
- decreased development risk;
- larger supplier market; and
- improved availability of parts.

However, the COTS approach is not without detractors, especially in a nuclear control system application. The main disadvantage is that many COTS items are not developed with the robust reliability and fault tolerance attributes that are essential to success. However, as will be seen with SIRCIS, the key is to integrate multi-level fault tolerant protection into the system.

IV. OASES CAT III STANDARD

The standard for the development of real-time protective, control and monitoring software in Ontario CANDU nuclear power plants is the Ontario Power Generation and Atomic Energy Canada Limited Software Engineering Standard (OASES) [1]. Although the OASES standard was developed with CANDU plants in mind, it was considered that the standard was scalable to meet the needs of a much smaller reactor such as SLOWPOKE.

There are four standards in the OASES family and they are defined as Categories I through IV. Category I is deemed to have the most significance to safety while Category IV is deemed to have no significance to safety.

There were two approaches that were contemplated for categorization. The first approach was that both control and instrumentation would be integrated together into one package. The categorization for the product would be attributable to whichever of the two aspects rated a high category, in this case, control. The other approach was to split control and instrumentation functionality into separate entities and apply only the lowest applicable category to each. In all likelihood, control would be Category III whereas instrumentation would be Category IV and require considerably less effort. In the end, it was decided to administer one standard (Category III) for the entire upgrade, thus assuring that both functions of SIRCIS were subjected to a clear, precise and rigorous development process.

V. DEVELOPMENT OPTIONS

Three potential paths for the development of a new digital control and instrumentation system for SLOWPOKE were originally considered. They were:

- development by a third party external to the university;
- development in partnership with a third party; or
- development entirely in-house at RMC.

Only the last two paths were explored further as the budget for a turnkey solution from a third party would have been expensive relative to the worth of the reactor and was thus not feasible. Considering that the original cost of the reactor in 1985 was ~ $1.3M, a new replacement console (in 2001) could be about $0.5M.

The obvious choice for a third-party solution was with the original reactor vendor – AECL. Their proprietary language called PROTROL (PROtection

and conTROL) had been successfully used in numerous nuclear applications including:

- DFCS (Digital Feedwater Control System) at Peach Bottom (2x1000 MWe BWR) Atomic Power Station owned by Philadelphia Electric Co;
- DFCS and DRCS (Digital Recirculation Control System) at Oyster Creek (680 MWe BWR) owned by GPU Nuclear;
- Neutron Generator Control and Safety Interlock System for KFUPM (King Faud University of Petroleum & Metallurgy), Saudi Arabia;
- Reactor Control and Safety System Upgrade, Pennsylvania State Brezeale Reactor (PSBR), Pennsylvania State University; and
- several real-time control system testbeds (running real-time models of Maple X10, Oyster Creek (BWR), etc.), in use at AECL at AECL-CANDU and CRNL [2] .

In addition, the SLOWPOKE Energy System (SES) was also considered a candidate for PROTROL [2] before the SLOWPOKE Demonstration Reactor (SDR) was shut down in 1989.

Most of these systems were developed in the late 1980's and they typically used 80286 or 80386 Intel processor computers with clock speeds between 6 and 20 MHz. PROTROL programs were developed in Pascal and run under a DOS operating system. The interfacing hardware that is supported by PROTROL is Computer Products Inc. RTP I/O product or Opto-22 I/O.

Another choice was Siemens Moore's QUADLOG® Safety System. This is a Programmable Logic Controller (PLC) that can be integrated with another of their products, called the APACS+® Process Automation System, in order to provide an integrated control and/or instrumentation system. This combination is being used extensively for the MAPLE reactors that were built for Nordion Ltd. by AECL at Chalk River Laboratories (CRL). In addition, the QUADLOG/APAC+ system is being implemented at the AECL NRU (Nuclear Research Universal) reactor at CRL. Since AECL CRL has already extensively qualified and developed two different reactor control systems using these products, it may have been possible to take advantage of the lessons learned to speed development of SIRCIS.

The third choice examined was National Instruments (NI) LabVIEW (Laboratory Virtual Equipment Workshop) product and their Signal Conditioning eXtensions for Instrumentation (SCXI) system. In 1990, a previous graduate student developed a software based SLOWPOKE-2 simulator at RMC as part of a M.Eng. thesis in Nuclear Engineering. He used a first generation LabVIEW product to create his reactor simulator and demonstrated that LabVIEW was a viable development system for control [3]. If LabVIEW were to be used again, then it might be possible to incorporate portions of the simulator into an operator trainer that could be used to transition Licensed Operators to SIRCIS.

An analysis of the three solutions was conducted and concluded that National Instruments products were best suited for SIRCIS development at RMC. The Siemens-Moore approach was a close second choice, and was just as valid a contender as the NI option. However, as NI products were already being used at

RMC, it made sense to choose this approach.

VI. OS AND HARDWARE OPTIONS

There are several commercially available computer operating systems (OS). Some have been around for a while and some are quite new. The OS is considered to be a critical component for any computer system. Its stability and effectiveness is paramount to system operation.

There are essentially two types of real-time operating systems: hard and soft. A hard real-time OS guarantees event timing within a certain interval while soft real-time systems cannot. The majority of personal computers have these general purpose, soft real-time systems. While there are COTS hard real-time OS environments available, the SIRCIS problem domain does not require such determinism due to the relatively slow changing processes within SLOWPOKE. Thus it was decided to use a general purpose, soft real-time OS.

The operating systems that work with LabVIEW were examined and Mac OS 9 was found best suited for implementation in SIRCIS. Microsoft Windows 2000 was also a reasonably strong contender, but was not the first choice.

Once the OS was chosen, AECL's Guide for the Qualification of Software Products [4] was used to ensure that the chosen commercial software was of sufficient quality for use in this particular application and categorization.

The computer hardware decision became relatively simple since the OS is only supported on computers manufactured by one manufacturer, Apple Computer. While it may seem a design weakness to sole source supply of the control computer to one manufacturer, a closer examination revealed that there are positive benefits. For example, the Mac OS is tightly integrated with the Apple hardware, since the hardware manufacturer and the software developer are contained in the same company. This level of integration is not always possible in the Windows and Intel (WINTEL) environment.

Another consideration was that, once computer hardware has been chosen, the control computer cannot be arbitrarily switched once the system is validated. That is, once a specific model of computer is validated, introducing a new (albeit similar) computer would likely necessitate repeating major portions of the test procedures. Therefore, a decision to source with one manufacturer would more than likely necessitate staying with that manufacturer and product. The key to mitigating the risks associated with a sole-source supplier is to shelve spares that are adequate to meet the maintenance requirements for the intended life of the product.

While there are several types of computers manufactured by Apple (e.g., portables, desktops etc), it was decided to use the most powerful desktop available at the time. This was the 500 MHz Power Mac G4. A cursory review of hardware specifications for the control computer verified that there should be no problem meeting computing performance requirements as specified in the requirements documentation.

VII. HUMAN FACTORS ENGINEERING

After an extensive review of SLOWPOKE-2 literature and familiarization with existing hardware, a prototype design was developed. This initial design was shown to operators on several occasions in order to receive their input, especially with respect to the MK2 console and how this next generation of control system should evolve.

There is no unique Canadian HFE standard used in the design of CANDU nuclear power plants. Rather, the Canadian nuclear industry relies upon the American Nuclear Regulatory (NUREG) Commission (NRC) standard, and to a smaller degree on IEEE standards. It was decided that, for SIRCIS, the NUREG standards would be considered the primary standard while the IEEE documents would be used strictly for comparison. The HFE Design & Implementation Process outlined in NUREG-0711 was followed in order to expedite HFE work.

These standards were not implemented rigorously as they were considered to be too onerous for such a small reactor as SLOWPOKE. Rather, the spirit of the standard and guideline were followed in order to ensure a logical and coherent approach to the task. The design standards that were consulted were NUREG-0700 Vols. 1 & 3 [5,6] and IEEE Std 1289-1998 [7].

VIII. SIRCIS OVERVIEW

Most SIRCIS components are housed in a 19” rack mount cabinet that is located in the control room. The rack contains the necessary hardware for SIRCIS. A 22” flat panel display (Figure 2) is located adjacent to the rack at the operator workstation. The operator interacts with the system using an optical mouse; there is no keyboard input.

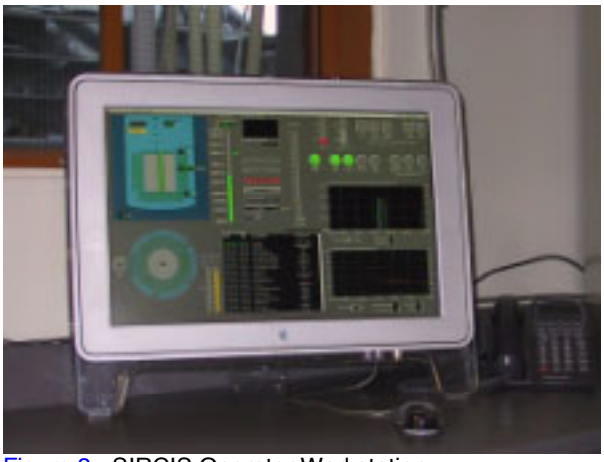

Figure 2 - SIRCIS Operator Workstation

IX. COTS ENHANCEMENTS

As mentioned earlier, the main disadvantage with COTS items is that many are not developed with the robust reliability and fault tolerance attributes that are essential in a nuclear application. The key to success is to build in multi-level, fault tolerant protection.

It is important to understand the terms, Fault Tolerance and Graceful Degradation, as they apply to computer control systems. Fault Tolerance is the built-in capability to provide continued correct execution, such as the provision of service as specified, in the presence of a limited number of hardware or software faults [1]. Graceful degradation is a stepwise reduction of functions in response to detected failures while essential functions are maintained [1]. One way to achieve these goals is

through redundancy, which is the presence of auxiliary components in a system to perform the same or similar functions as other elements for the purpose of preventing or recovering from failure. Fault tolerance and graceful degradation features that are found in SIRCIS include:

- redundant displays
- redundant hard drive storage
- hot swappable input device
- triple redundant power supply
- gravity-based control rod insertion

In SIRCIS, three watchdogs are used to provide redundant “health” monitoring of applications and processes such as:

- the main application;
- the Operating System; and
- the process.

The third watchdog monitors SIRCIS processes to ensure that they operate uninterrupted. The program must regularly reset a hardware counter to prevent it from "barking" (expiring). This must occur in less than 0.5 seconds or a power relay will be opened causing a gravity-based control rod insertion. The power relay is also opened if power to the SCXI or control computer fails (e.g., blown fuse, electrical short, etc.).

This triple redundant approach to health monitoring ensures maximum reliability and availability of the system. This is especially important during remotely attended operation when no Licensed Operator is required to check on the system for periods of up to 24 hours [8].

Should SIRCIS fail to operate properly, the operator can also trip the reactor by turning a key switch that controls the power to the control rod motor. The control rod would then undergo a gravity-based control rod insertion into the core and the reactor would shut down.

Although SIRCIS has some redundancy and fault tolerance capabilities, it is important to note that there are single points of failure within SIRCIS. For example, there is only one DC power supply, one computer, one data acquisition chassis and a single neutron flux channel. A failure of any one of these items would result in varying degrees of failure within SIRCIS. It must be understood that this is the same situation as with the MK2 control system, and does not represent a departure in design philosophy. The safety of the reactor does not depend on the control system, be it analog or digital; it relies upon the physical characteristics of the reactor to make it inherently safe.

X. VALIDATION AND VERIFICATION

All work for SIRCIS was conducted with a view towards eventually receiving permission from the Canadian Nuclear Safety Commission (CNSC) for the implementation of SIRCIS. An independent third party conducted the Validation and Verification phase in order to satisfy the requirements for the Category III standard [1]. A contract consisting of documentation review and system testing was awarded to an experienced software testing company.

To aid in this effort, a test stand (Figure 3) consisting of a full-scale cut-away model of the SLOWPOKE-2 reactor was instrumented with the required

hardware. The reactor model, previously used to promote sales of SLOWPOKE reactors when it was a commercial product, is shortened in the vertical scale to approximately 2 m in height. A 19" rack was used to house the control computer, UPS, SCXI hardware and test stand wiring panel. The test stand was also useful for practicing installation and maintenance procedures, and in the future will be used for reactor operator training and demonstrations.

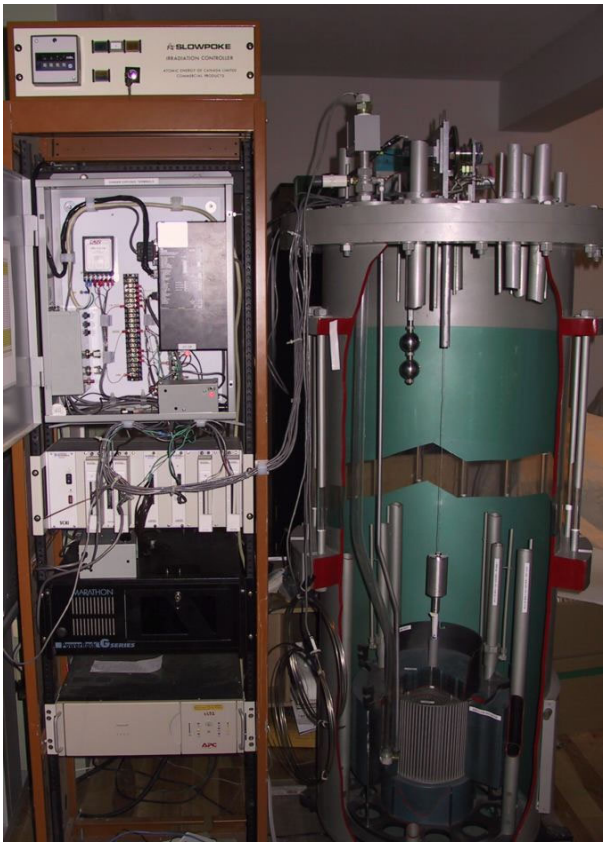

Figure 3 - Control System Test Bed

Once V&V efforts were successfully completed, the test stand was moved back to RMC in April 2001 where further trials were conducted pending approval of the Commissioning Plan that had been submitted to the CNSC.

REFERENCES

[1] OASES, COG-95-264-I Rev 1.0, "Software Engineering of Category III Software", 1995.

[2] Fournier, R. David, "PROTROL™: A Modern Industrial Micro Based DCC System", AECL CANDU, October 1990.

[3] Cottingham, G.P., "A Real-Time Simulator for the SLOWPOKE-2 Nuclear Reactor at Royal Military College of Canada", April 1990.

[4] COG-95-179-I Qualification of Software Products.

[5] NUREG-0700, Rev. 1,Vol. 3, "Human-System Interface Design Review Guideline – Process and Guidelines", U.S. Nuclear Regulatory Commission, June 1996.

[6] NUREG-0711, "Human Factors Engineering Program Review Model", U.S. Nuclear Regulatory Commission, July 1994.

[7] "IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Generating Stations", IEEE Std 1289-1998, IEEE Power Engineering Society, May 1998.

[8] RMC Research Reactor Operating Licence, Atomic Energy Control Board, 13 October 1999.