The Role of Automated Testing and Logging Tools in Fuel Handling I&C Refurbishment: Bruce A NGS FH Protective Replacement

Jeremy Dalby[1], Yvonne Mackwood[1], Walter Volk[1], and Wendy Yu[2]
[1] GE Hitachi Nuclear Energy Canada, Peterborough, Ontario, Canada
(walter.volk@ge.com)
[2] Bruce Power, Tiverton, Ontario, Canada

Abstract

The replacement and upgrade of nuclear-related I&C systems forms an important part of the refurbishment and life extension of the CANDU fleet. Replacement of the DEC PDP-based fuel handling Protective computer at the Bruce A NGS has brought with it challenges in both design reimplementation, and in ensuring a smooth path through installation and commissioning. In order to achieve success, innovative approaches to in-field data logging and automated testing equipment for PLCs were needed. GEH-C's Automated Software Test Equipment and datalogger (ASTE/d) has been a key tool in ensuring verification and validation of replacement designs, test repeatability, and enhanced coverage, while contributing to project cost and schedule adherence.

1. Introduction

Control and monitoring systems which are key to the safe and efficient operation of the CANDU fleet today depend upon instrumentation, field transducers and computational control components, many of which represent the original equipment installed in plants 20, 30 or 40+ years ago. In some cases, CANDU plants have undergone major refurbishment cycles (e.g. reactor retubing) without the replacement or upgrade of I&C systems integral to critical production systems, such as the online fuelling control and protection systems. Stations are coming to terms with a significant proportion of system failures and downtimes due to functional failures of I&C components; in some cases representing two-thirds of the total proportion of system component failures. In addition, these plant components are considered an opportunity for major improvement in preventive maintenance programs [1].

Aging, legacy I&C systems bring with them particular challenges in their upgrade or replacement. The design documentation produced during their original development is often lacking a level of rigour commensurate with systems designed today under modern hardware and software development practices and standards. The retirement of subject matter experts (SMEs), or discontinuance of the original equipment manufacturer (OEM), stifle the search for design knowledge and details beyond that existing in the surviving documentation. Often times "the devil is in the details" and these details are only to be found in the subject system in the field!

Additionally, the integrated and interdependent functionality of some nuclear-related I&C systems poses significant challenges in replacement logistics, especially if performed out-of-sync with major plant refurbishment projects. System down-time required to accommodate upgrades, or the installation of an entire replacement system, may directly affect plant production as in the case of

the fuel handling system. Operations and Maintenance's familiarity with the new system, and confidence in its validation and performance as a fully functional replacement for the legacy system, may require considerable 'online' time to accomplish. Any validation that can be accomplished earlier in the design life-cycle (especially ahead of the installation and commissioning phases) builds confidence in the new system's functionality. This is also economically beneficial to the project and represents a significant mitigation for late, in-plant discoveries.

Successful I&C replacement and upgrade projects share common measures of success with other refurbishment endeavours: the achievement of all technical (and safety) requirements, within budget and schedule. Tooling, innovation, and methodologies that can be applied to achieve these goals in a productive and economical manner, in the presence of the challenges described above, will ensure the success of the refurbishment and life extension of the CANDU fleet. GE Hitachi Nuclear Energy Canada's (GEH-C) Automated Software Test Equipment and datalogger (ASTE/d) represents such an achievement for the Bruce A NGS Fuel Handling (FH) Protective computer replacement project.

2. Background

The Bruce A FH system comprises three mobile, trolley-based fuelling systems serving Units 1 through 4 at the station in Tiverton, Ontario. The trolley systems, fuelling machine heads, reactor and Central Service Area bridges are capable of supporting on-power refuelling, and transporting new and irradiated fuel between the reactor channels and storage bays. They are independently operated via an I&C system, separate from the reactor controls.

The Bruce A FH I&C system was designed in the late 1960's, incorporating then state-of-the-art Digital Equipment Corporation (DEC) computers. Each independent FH control system comprises a PDP-8/E "Controller" computer and either a PDP-14 or PDP-8/E "Protective" computer. Although all of the FH computer equipment is now obsolete and functioning beyond its original design-life, a decision was made to begin with replacement of the Protective computers only, in order to reduce project risk and minimize operational impact [2]. At the outset of 2012, Bruce Power and GEH-C initiated the start of design work to replace the Bruce A FH Protective computer system.

The FH Protective is a COG Category 2 safety-related system [3]. Its primary task is to monitor equipment motion orders issued by the Controller computer and/or operator manual console inputs, and evaluate whether current field conditions allow for the motion to be safely realized. The Protective software is written entirely in assembly language and represents over 250,000 total lines of code which has continued to evolve over 35 years of operation in service.

Replacement of the FH Protective computer system represents a "first-of-a-kind" (FOAK) project for Bruce Power, and a "first-in-a-while" (FIAW) project for GEH-C. FOAK I&C replacement projects such as this typically involve significant changes in their reimplementation of legacy functionality. Due to the scope of these modifications, it is often necessary to perform an impact assessment to identify required changes to the original design basis and validate these in the final system.

Early in the project life cycle, GEH-C recognized the need for unparalleled levels of verification and validation to ensure successful project execution, and planned to address this need through automated testing, data collection and analysis. With this in mind, ASTE/d was conceived and represents a considerable enhancement to traditional testing methods, as it affords the capability to monitor and analyze the detailed execution behaviour of an I&C system, and eases the execution of testing at multiple levels, in a cost- and time-effective manner.

3. Design and Implementation Challenges

The key objective of the Protective computer system replacement is to re-implement the central DEC control hardware and software such that the replacement PLC-based system is functionally equivalent to the existing legacy system. To successfully achieve this objective, it was imperative to understand the functional and dynamic behaviour of the installed system, and to define and document the detailed requirements completely and correctly to describe the behaviour of the legacy hardware and software. Given the era of its development and the state of engineering standards and processes available at the time, formal mathematical design specifications were never developed, though fault tree analysis techniques were attempted in later years [4].

3.1 Lack of Subject Matter Expertise

The original developers of the legacy Protective computer system have long since retired, and only a few engineers remain who have worked with the legacy FH I&C system long enough to become SMEs. The resulting paucity of engineering expertise often drove a need for lengthy investigations to determine the details of specific system behaviours that might otherwise have been elicited by a short conversation with an SME.

3.2 Incomplete Legacy Documentation

The legacy software was designed and implemented following old design standards that did not require development of a thorough documentation set in accordance with currently accepted nuclear I&C design standards. Although effort was subsequently made to upgrade portions of the documentation, it remained incomplete at the onset of the Protective computer replacement project. Modifications and functional enhancements to the FH system evolved the Protective computer design further over the 30+ years that the plant has operated. However, as is often the case with legacy designs, updates to design documentation have not always been diligently or uniformly executed. Gaps, unintentional errors and inconsistencies have resulted from the accretion of iterative design changes. It was therefore not possible to rely entirely on the legacy documentation when defining the replacement requirements.

3.3 Reverse Engineering from Source Code

To fill the gaps and validate the information within the legacy documentation, a complete read through of the legacy software source code was performed. The legacy software is written entirely in assembly language containing inline comments which are constrained by the language structure. This causes the source to be difficult to read and reverse engineer into requirements, particularly for newer engineers who are less versed in assembly language programming, and are new to the legacy DEC computer system. Even after comparing the legacy documentation against the legacy software source code, further validation methods were required to ensure that the subtle nuances of the executing software were captured correctly in the design requirements.

3.4 Software Errors

In January 1990, an incident occurred at Bruce A in which the bridge supporting a fuelling machine attached to channel C08 on unit 4 unexpectedly lowered, causing the weight of the fuelling machine to be supported solely by the channel end fitting. This resulted in end fitting deflection causing a significant leak of heavy water from the reactor's primary heat transport system [5].

Subsequent investigations revealed that the Unit 4 C08 incident occurred in part due to a Protective computer software error that had lain dormant in the software for several years, demonstrating once again that in a complicated I&C system, some programming errors are not necessarily revealed in extensive use [6]. A particular fault, latent in the subject system, may indicate its presence only under very specific operating or environmental conditions.

Rigourous formal verification and exhaustive test coverage afforded by automated tooling and techniques can be key to improving I&C quality. These activities reduce the likelihood that software errors arising from incorrect design requirements and/or the software implementation process will escape to the fielded system.

4. ASTE/d Strategy

Given these design and implementation challenges to the successful replacement of the DEC Protective computer system, GEH-C and Bruce Power sought to develop a transportable, multipurpose I&C test and development tool that could provide the engineering team and plant with facilities that would benefit each phase of the development life-cycle. Legacy system design investigation, requirements development, detailed design, implementation, testing validation and commissioning would all benefit from the power of data collection, analysis, and automation.

With this strategy in mind, ASTE/d was evolved as a single physical platform (Figure 1) which, with minor hardware reconfiguration and a library of software applications, could accomplish the following three key functions:

- Field data logging;
- Logged data playback;
- Scripted testing.

Figure 1: ASTE/d Physical Package

The implementation of ASTE/d was driven by certain critical characteristics, including an emphasis on automation to reduce project labour costs, and a design to allow for certification as a qualified testing tool to the guidelines of IEC 60880 2006-05 and CSA N290.14-07. Cost and schedule were also key considerations, as ASTE/d development costs would need to be significantly less than the main I&C replacement project, and the tool had to be available for service early in the project to maximize its benefit to the project at large.

4.1 Field Data Logging

Gaps in the detailed understanding of the function and dynamic behaviour of the legacy computer system and field equipment presented significant challenges in defining and verifying detailed I&C requirements in order to ensure that they completely and accurately represented the legacy Protective system behaviour. Though many of the details of static logic could be gleaned through careful examination of the legacy software source code, further measures were needed to ensure that all functions, including subtle nuances and system dynamics, would be identified and documented correctly.

To arrive at a complete and accurate picture of the interaction between the legacy computer system and the field equipment, the best place to look was at the field inputs and outputs (I/O) of the system in-situ. Due to the large volume of field I/O and the frequent, short duration state changes, real-time observation of signals by a human was not feasible. Instead, field I/O signals must be sampled at a high frequency and recorded to file such that off-line examination and analysis could be performed. This was made possible by the ASTE/d data logging function design.

When configured for field data logging, the ASTE/d continuously reads the states of up to 832 digital inputs and 8 analog inputs in real-time, and records their states within a non-volatile data log file. As depicted in Figure 2, all field input and output signals of the legacy FH Protective computer were electrically split and isolated, allowing connection to the ASTE/d inputs without interfering with fuel handling operations. Once set up and initiated, data logging could proceed non-intrusively and unattended during normal system fuelling operations at Bruce A NGS.

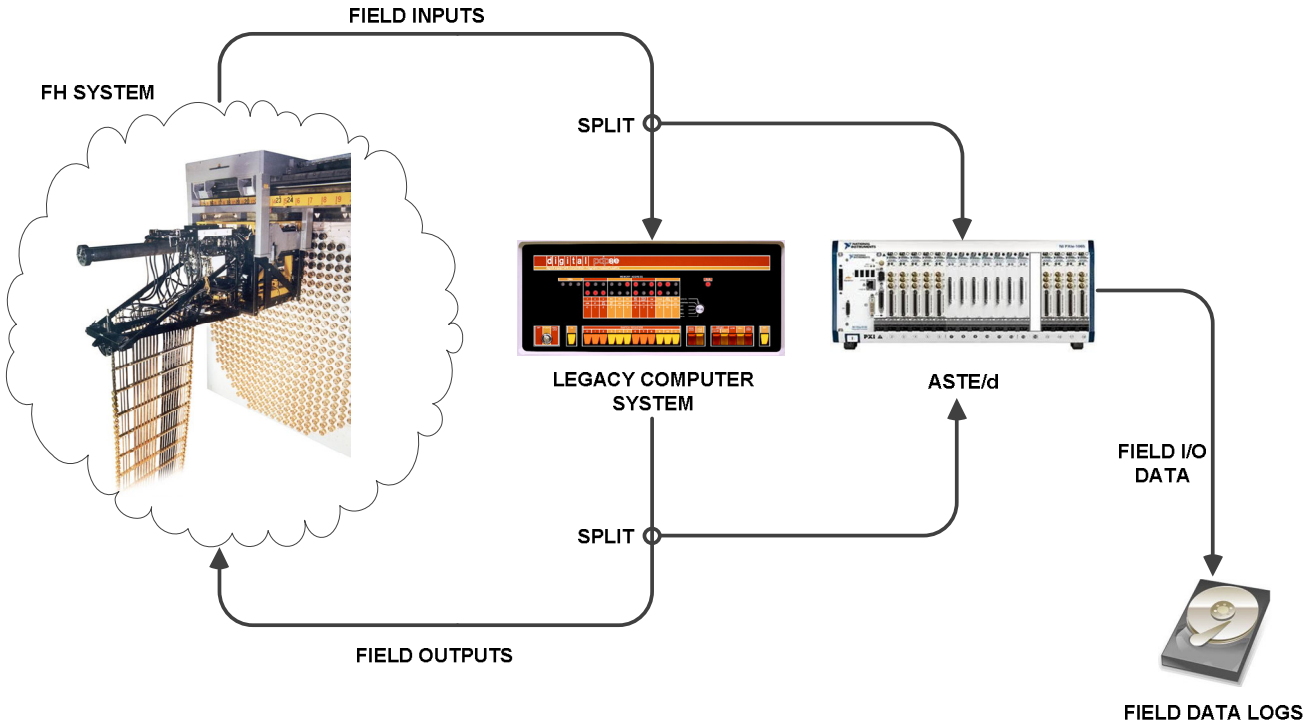

Figure 2: Field Data Logging Topology

In parallel with preliminary design activities, three months of aggregate in-plant logging by ASTE/d was conducted to gather the dynamics of the legacy Protective computer system in active fuelling, on multiple trolley systems. The data collected by the ASTE/d provided a detailed picture of the dynamic I/O behaviour of the legacy FH Protective computer, as well as the behaviour of the field equipment connected to it. This data was then used during early phases of the project to validate critical software requirements and to mitigate gaps in the existing design documentation and the lack of SMEs.

4.2 Logged Data Playback

While the collection of significant volumes of 'live performance' of the legacy I&C system represented a valuable asset to the early requirements, design and implementation stages of the project's development life-cycle, a very powerful opportunity existed to re-apply this data-set to the actual implementation to evaluate and validate how the integrated replacement solution matched the legacy system under simulated field conditions and scenarios. This capability would then serve to bring the in-plant system into the testing and validation laboratory, and provide design engineers and plant operations a preview of replacement system operation under field conditions. As such, the ASTE/d data playback function was designed to be capable of providing this ad hoc simulation capability, with an appropriate level of fidelity, and at significantly lower project costs than full system simulator tooling.

When configured for logged data playback (Figure 3), the ASTE/d reads the field input states previously recorded within a data log file and applies them as digital and analog output signals connected to a replacement computer system under test. Concurrently, ASTE/d also reads and records the output signal states of the system under test for comparison with the outputs recorded by field data logging performed at the plant.

All logged data playback activities proceed in real time, identical to field data logging.

Following logged data playback, the outputs of the legacy computer system are compared against the outputs of the replacement computer system in response to the same computer system inputs using PC-based automated data comparison tools. Differences outside of tolerance between the behaviour of legacy computer system outputs versus replacement computer system outputs are summarized within an automatically generated inconsistencies report. Each inconsistency within the report is investigated and analyzed by engineering and system SMEs to ensure there is a complete understanding of the behavioural differences, and that appropriate corrections are applied to the design implementation.

After implementing all required software and hardware corrections discovered during the first pass, logged data playback is repeated. The process is iterative, concluding when only a short list of well understood, acceptable observations remain, agreed between design and plant engineers. This provides a high degree of confidence that the replacement computer system is functionally equivalent to the legacy computer system in both requirements and implementation.

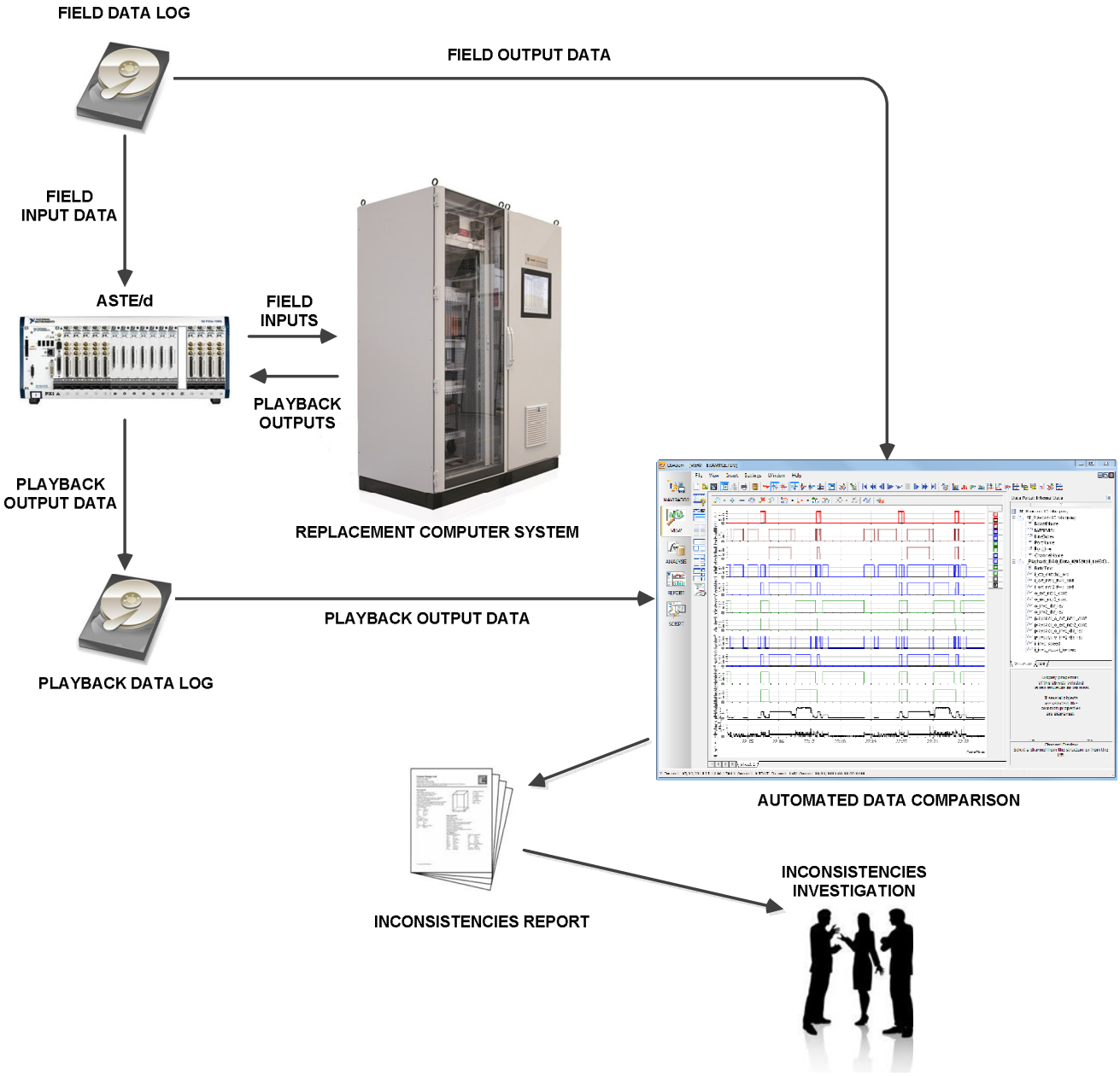

Figure 3: Logged Data Playback Topology

One limitation of field data logging and playback is that the majority of scenarios captured as data logs represent normal system operation. Many of the abnormal system operation scenarios cannot feasibly be recorded at the station since to do so would require putting the field equipment into situations that are potentially unsafe or may cause damage. To overcome this limitation, it is possible to edit the data log files to inject abnormal system operation scenarios. The modified data log files can be played back against the replacement system to verify correct behaviour. The data log editing process is, however, somewhat labourious, which renders this approach an expensive option for extending test coverage.

4.3 Scripted Testing

Design defects, when discovered early in the design process, cost significantly less to correct than those discovered in subsequent phases. With this in mind, GEH-C and Bruce Power recognized the importance of developing the capability to support rigourous formal verification and exhaustive test coverage early in the project design life-cycle. This test approach also provided the best chance of detecting latent, potentially catastrophic software defects, which may not otherwise be revealed even after many years of extensive in-service usage.

While the combination of field data logging and playback verified that the replacement FH Protective behaves correctly during normal system operations and a limited number of abnormal system operations, numerous scenarios remained untested. To achieve this additional testing coverage, hundreds of test cases would need to be defined and executed. Though technically feasible to verify all scenarios by playing back modified data log files, an inordinate amount of effort would be required to create the modified data log files and analyze the playback results. Similarly, the vast number of test cases and field I/O rendered manual testing infeasible and nearly impossible to execute repeatedly without human error. To complete the intended testing program in a cost- and time-effective manner, the need for a tool that supports automatic execution of easy-to-create test cases quickly became apparent. This led to the development of the ASTE/d scripted testing function.

When configured for scripted testing (Figure 4), the ASTE/d automatically executes a sequence of scripted test cases, each of which defines a functionally significant combination of computer system field input states and the expected field output states. The field input states defined by each test case are electrically presented to the replacement computer system under test, and the resulting actual field output states are monitored and compared against the expected field output states defined in the test case. Each test case is deemed a "pass" if the actual field output states match the expected field output states upon execution by the system under test. The results of each test case are recorded in a test report automatically generated by the ASTE/d.

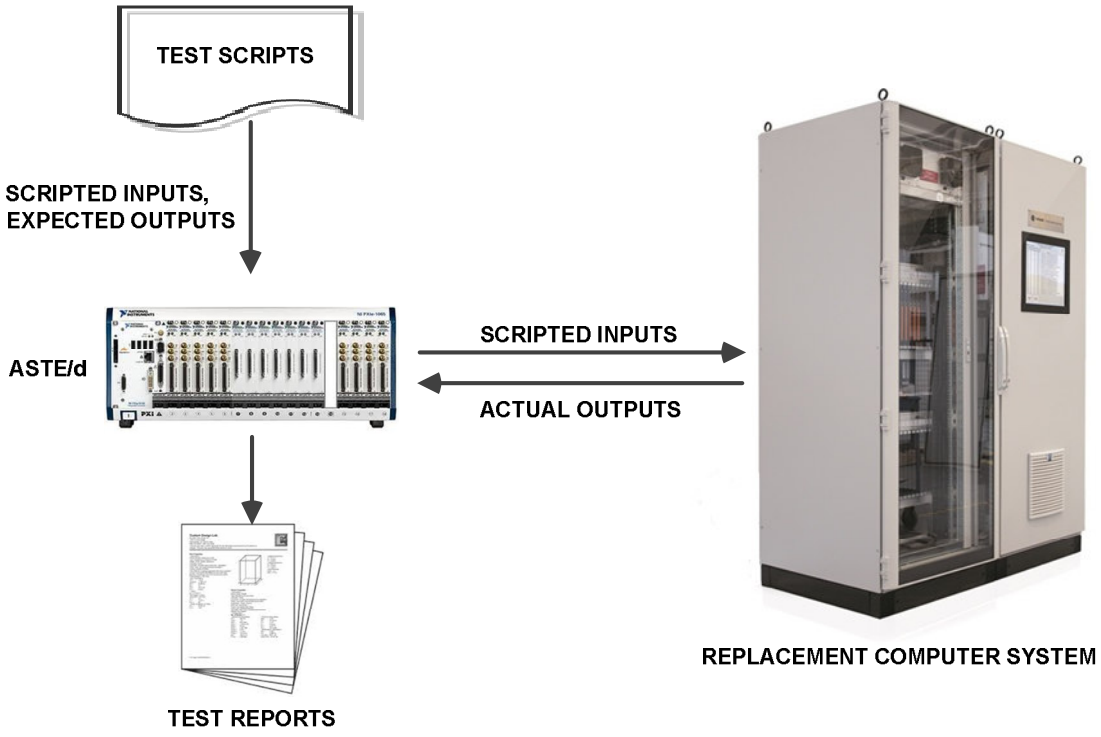

Figure 4: Scripted Testing Topology

Automated scripted testing using ASTE/d offers numerous advantages over manual testing:

- Test execution proceeds unattended, which eliminates most labour costs associated with test execution;
- Automated tests are executed in exactly the same manner every time, guaranteeing test repeatability and eliminating the potential for human error in test execution;
- Automated test execution can take place at any time (including evenings and weekends), which frees up equipment to be used for other purposes during regular business hours;
- Many test cases can be executed in a short and predictable amount of time, thereby contributing to project schedule adherence;
- Test results are automatically analyzed and summarized within a test report that can quickly and easily be assessed by engineering staff, and serves as an audit trail of verification activities;
- Additional testing capacity can be afforded by acquiring additional ASTE/d and system under test equipment, usually with only a modest capital impact to the project;

- It is often cost- and time-effective to execute the entire suite of test scripts following software modifications, rather than selecting a subset of tests to execute as a regression suite. This reduces the risk of missing unintended or misunderstood side-effects of software modifications in the regression analysis.

High-speed testing using ASTE/d's automated scripted testing function reduces test execution time constraints, affording the possibility of executing a comprehensive suite of test scripts that achieve additional path coverage, which reduces project risk. In addition, the ease with which an entire suite of test scripts could be executed following software modifications, rather than selecting a subset of tests to execute as a regression suite, and the comparatively small project cost and time impact of doing so, often made the former the practical choice. In doing so, the common risk of missing unintended or misunderstood side-effects of software modifications in the regression analysis was substantially reduced.

4.4 Flexible Configuration

For the FH Protective computer replacement project, ASTE/d was also designed with the flexibility to execute scripted tests using either a hard-wired I/O interface with the replacement I&C system, or over a networked data highway, bypassing the I/O subsystem of the computer system under test.

When configured for use without the I/O subsystem, the ASTE/d emulates field I/O via a Modbus/TCP Ethernet communication link such that no digital or analog I/O modules are needed for the ASTE/d or the replacement computer system. This configuration allows for software test execution to proceed prior to the availability of a complete computer hardware setup. Software non-conformances can be identified and corrected early in the development life-cycle, thereby reducing project costs associated with software development. This configuration also reduces the capital cost of development laboratory testing, since its setup requires no hardware I/O subsystems and the ASTE/d needs only a standalone PC.

When configured with a hardware I/O subsystem, the ASTE/d drives and monitors field I/O via a collection of electrical signals, each individually wired between I/O modules on the ASTE/d and the replacement computer system. This configuration is ideal for testing the computer system with integrated hardware and software.

Since the same test scripts can be used for both ASTE/d configurations, it was possible for many of the test scripts written for software testing to be reused during integration and system functional testing of the FH Protective computer replacement project, contributing to reduced testing costs, and ensuring both schedule adherence and confidence in equivalent software functionality to the legacy system.

5. Conclusion

The conception and successful use of GEH-C's ASTE/d multipurpose I&C test and development tool during the Bruce A NGS Protective computer replacement project demonstrated the key role that automated testing and logging facilities can play in solving a number of issues characteristic of legacy I&C replacement efforts in CANDU plants today. Mitigating the common gaps in subject matter expertise, legacy system documentation and understanding, original design basis impact and the inherent challenges of FOAK/FIAW engineering endeavours, ASTE/d demonstrates key opportunities to reduce development risk, improve I&C product quality, and contribute to project cost savings and schedule adherence. Tooling, innovation and methodologies, like those collaboratively applied by Bruce Power and GEH-C to this project, will contribute to the success of plant refurbishment and life extension efforts.

6. References

[1] M. Darragi, D. Komljenovic, R. Vaillancourt and M. Croteau, "Preventive maintenance optimization at the Gentilly 2 NGS: initial results and lessons learned", 7th International Conference on CANDU Maintenance, Toronto, Ontario, Canada, 2005.

[2] M. Madani, J. Giajnorio, T. Richard, D. Ho, W. Volk and A. Ertel, "Program planning challenges for control system upgrades", 9th International Conference on CANDU Maintenance, Toronto, Ontario, Canada, 2011 December 8.

[3] G.H. Archinoff, D.K. Lau, J. de Grosbois and W.C. Bowman, "Guideline for categorization of software in nuclear power plant safety, control, monitoring and testing systems", Chalk River Laboratories, COG-95-264 Revision 1.0, 1995 May 24.

[4] M. Nourani, W. Bowman, D. Levan and F. Kanji, "Fault tree analysis of software at Ontario Hydro", 12th Annual Conference, Canadian Nuclear Society, Saskatoon, Saskatchewan, Canada, 1991 June 9-12.

[5] Atomic Energy Control Board, "AECB Staff Annual report of Bruce NGS 'A' for the Year 1990", AECB Report INFO-0394, 1991 June.

[6] M. Nourani, D. Levan, F. Kanji, L. Bedford and D. Hanoir, "Bruce NGS A: Hazards analysis of the PDP-14 Protective fuel-handling software for spurious vertical motion of a clamped-on fuelling machine", Nuclear Safety Department Report No. 91026, 1991 March.