Test Rig Overview For Validation And Reliability Testing Of Shutdown System Software

M. Zhao, A. McDonald, P. Dick
Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

Abstract

The test rig for Validation and Reliability Testing of shutdown system software has been upgraded from the AECL Windows-based test rig previously used for CANDU6®[1] stations. It includes a Virtual Trip Computer, which is a software simulation of the functional specification of the trip computer, and a real-time trip computer simulator in a separate chassis, which is used during the preparation of trip computer test cases before the actual trip computers are available. This allows preparation work for Validation and Reliability Testing to be performed in advance of delivery of actual trip computers to maintain a project schedule.

1. Introduction

The test rig for Validation and Reliability (V&R) Testing of shutdown system software has been upgraded from the AECL Windows-based test rig previously used for CANDU6® stations. This upgrade takes advantage of current advances in computer technology, especially the technology of Data Acquisition (DAQ) cards.

The V&R test rig hardware used for the recent projects (Wolsong, Qinshan and Cernavoda) was composed of National Instruments (NI) DAQ cards made in early 1990's. These DAQ cards are obsolete and hence difficult to replace or repair. In addition, these legacy DAQ cards do not have on-board buffers to support hardware timing and triggering. They are supported by the traditional DAQ drivers only, not by NI new DAQ_{mx} drivers. The new NI DAQ cards with the new NI DAQ_{mx} drivers have better performance in terms of speed and reliability. Consequently there is a requirement to update the test rig hardware, which also has a spin-off benefit of improved performance.

The test rig software, ATLIN (AECL Test Language Interpreter), has the following main modules:

- Test Language Interpreter
- Virtual Trip Computer (VTC)
- Virtual Display Computer (VDC), and
- PDC Simulator (newly added)

The ATLIN software for these recent projects was based on an older version of the NI LabVIEW, a high-level graphical programming language. The timing was measured by software polling, which was affected by the Windows 95 operating system, the CPU speed, and inefficient LabVIEW programming structure limited by the early 1990's technology. A Logic Analyzer had to be used to confirm timing measurements. Therefore, the V&R test report had to include not

[1] CANDU6® is a registered trademark of the Atomic Energy of Canada Limited.

only the test logs and reports automatically generated by the ATLIN, but also the manual test results using the Logic Analyzer, causing inconsistency in format and low efficiency in preparation of the documentation.

The newer version of LabVIEW has an Event structure, which eliminates the software polling. This greatly improves the efficiency in running ATLIN. Together with the new DAQ cards and the new DAQ_{mx} drivers, the newer version of LabVIEW can perform hardware timing and triggering which greatly improves the accuracy of the timing measurement, hence eliminating manual use of the Logic Analyzer for shutdown system software trip timing measurements. Consequently these advances in NI technology led to a requirement to update the test rig software to be compatible with the new generation of NI DAQ cards.

Given the difficulty in maintaining the old test rig, the benefits to streamline testing documents, and achievements in improved timing measurement accuracy, it was concluded that an upgraded V&R test rig would be developed for the Point Lepreau Refurbishment (PLR) project.

2. Hardware Upgrade

For the new V&R test rig, the NI platform was again selected to minimize the impact on the existing V&R test scripts by using the same scripting language, thus reducing the schedule risk to update these V&R test scripts.

In addition, a new feature to the V&R test rig is a PDC Simulator designed to emulate the actual PDC, trip computer. This PDC Simulator is used in the development of V&R test scripts. It uses the exact same components as the V&R test rig, which provides a spare during actual V&R testing of the shutdown system software. It has also proven useful as a training tool for test script preparation.

The new V&R test rig hardware is composed of NI PXI (PCI Extensions for Instrumentation) system as shown in Figure 1. The NI PXI system was selected for the following reasons:

- Synchronization between all DAQ cards inserted into the PXI chassis is inherent. No additional means are required. This added the simplicity in the hardware and software design for both the V&R test rig and the PDC Simulator.
- Timing measurements are hardware-based, separate from the main software routine without using software polling and independent from the operating system, which is a great improvement from the previous Windows-based test rig. The measurement data are stored in the on-board buffers of the DAQ cards and processed later. This significantly increases the accuracy of the timing measurements and provides deterministic performance.

The controller installed on the left-hand side of the chassis is dual booting, from either a WindowsXP or a LabVIEW Real Time (RT) operating system. The V&R test rig is running on the WindowsXP operating system and the PDC Simulator on the LabVIEW RT operating system.

The custom I/O terminal blocks shown in Figure 1 have been designed for connecting to the PDC I/Os. The following means are used to protect NI digital DAQ cards:

- optical isolation has been built into the D/I terminal blocks to isolate 48Vdc power plane for PDC from 5Vdc for DAQ cards.
- digital buffering has been built into the D/O terminal blocks between the relay coils and the DAQ card.

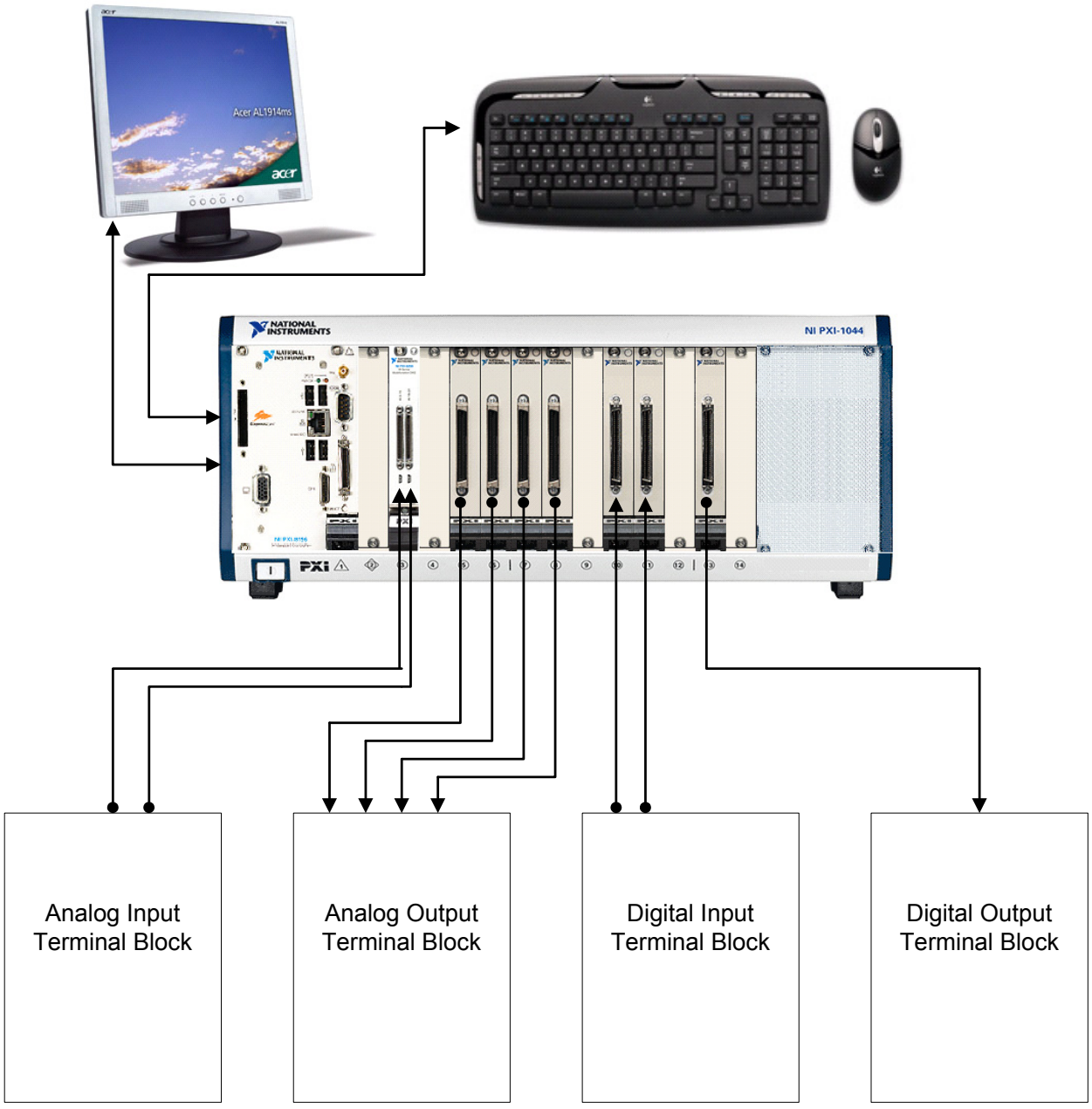

Figure 1 PXI DAQ Overview Layout

The SDS1 and SDS2 V&R test rigs are identical in both hardware and software. Each one can be used for V&R testing of either SDS1 or SDS2 shutdown system software. The PDC Simulator hardware is identical to the V&R Test Rig hardware and installed in the SDS2 V&R test rig with a switch selectable to emulate either SDS PDC. They are mounted in two 19" racks as shown in Figure 2.

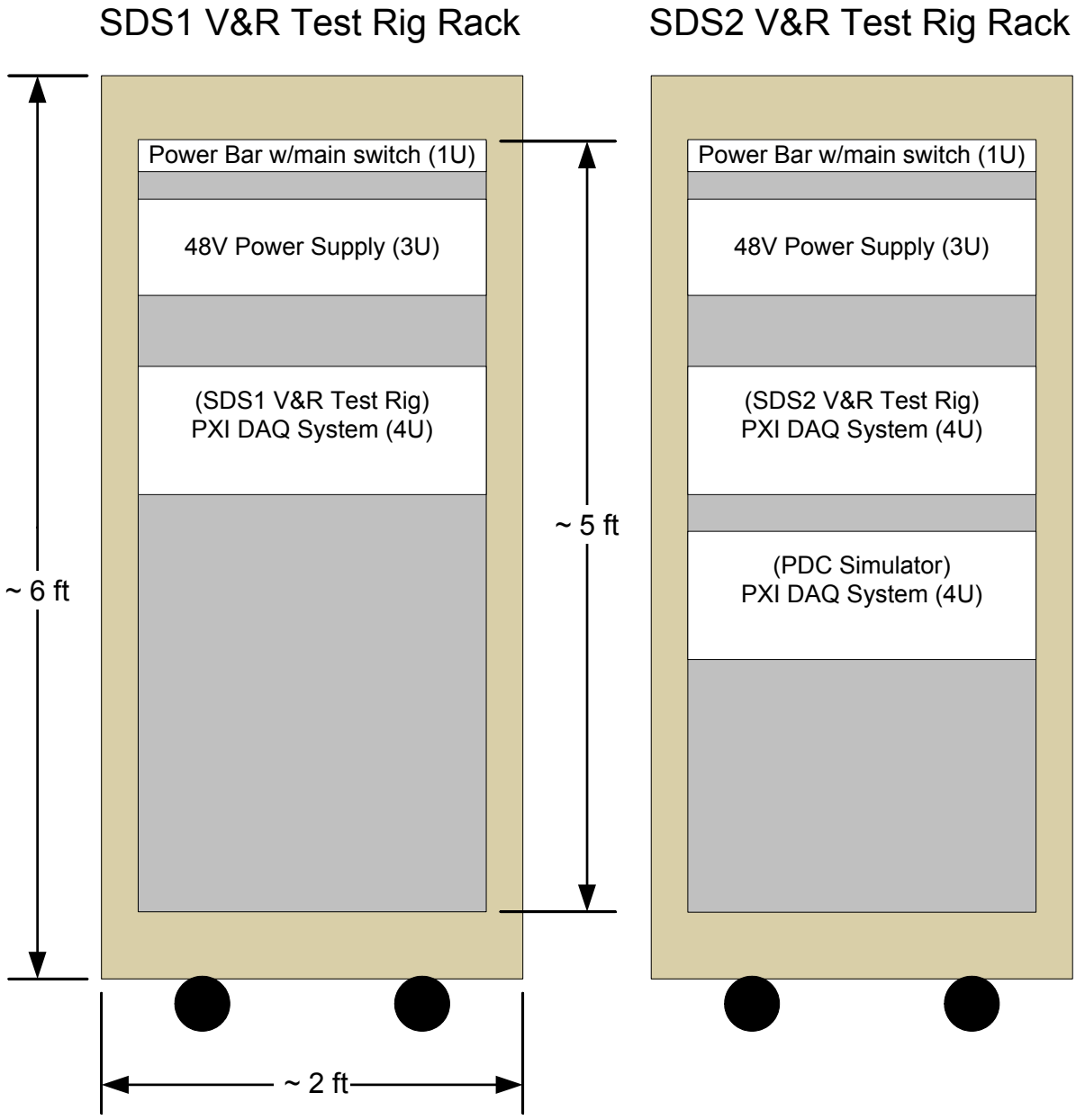

Figure 2 SDS1/2 V&R Test Rig Racks

The top chassis consists of a 48 Vdc power supply to be used for energizing the test rig and PDC digital inputs. The 48 Vdc voltage selected is the same as in the field installation of the actual PDCs.

The middle chassis consists of a NI PXI system with the controller running on the WindowsXP operating system. ATLIN runs on this NI PXI system to perform the V&R testing of the shutdown system software.

The bottom chassis in the SDS2 V&R test rig consists of a NI PXI system with the controller running on the LabVIEW RT operating system. This chassis simulates the actual PDC functionalities specified by the Trip Computer Design Requirements (TC DR) document. A switch is provided to allow the tester to choose which PDC to simulate, SDS1 PDC, SDS2 PDC1 or PDC2 (there are two PDCs for SDS2).

3. Software Upgrade

The new ATLIN is based on the NI LabVIEW 8.2 programming language. Use of built-in functions and structures in the newer version of LabVIEW makes the new ATLIN readable, scalable, and more easily maintainable.

The new ATLIN has similar screen appearance to the previous ATLIN user-interface. New functions have been designed and included in the new ATLIN based on previous test rig experience feedback. All previous functions have been maintained to provide convenience for staff familiar with the previous ATLIN.

The new ATLIN runs more efficiently using an Event structure only available in the recent versions of LabVIEW. It uses considerably less CPU time and does not need to poll the tester's keyboard inputs to determine the next execution. The software polling affected the accuracy of timing measurements and the speed of command execution in the previous ATLIN.

Together with the latest DAQ cards and their DAQ_{mx} drivers, the new ATLIN can provide hardware timing and triggering, which greatly improves the accuracy of timing measurements.

An important change in maintaining ATLIN software is that all PDC constants, I/O names, and I/O scales are stored in separate text files which are dynamically linked to ATLIN, i.e., no longer hard-coded in the ATLIN program. This is especially important for PLR project since the V&R test rig is developed in parallel with changes in design of the shutdown system and hence the latest design changes in the PDC constants, I/O names, or I/O scales can be easily incorporated without updating the ATLIN software, thus eliminating its re-qualification, which was happening on previous projects. This has proven to save time and avoided schedule slippage when the final design values for these parameters were given to the V&R groups.

4. Virtual Trip Computer

The Virtual Trip Computer (VTC) is an executable software version of the PDC functional specification located inside of ATLIN. When executed, it behaves like a software black box whose functions match with those specified in the TC DR. With the help of LabVIEW, the

conversion of the functional specification of an actual PDC to an executable emulator is easily reviewable by visual inspection.

The VTC is the reference used for Reliability Testing, which has the spin-off benefit of debugging the Validation test scripts developed independently of the ATLIN programming, and independently of the PDC software programming and hardware development. By running the Validation test scripts on the VTC first, the tester can correct bugs in the test scripts before performing the tests on the actual PDC. This allows preparation work for V&R Testing to be completed in advance of delivery of actual PDC, target computer, to maintain a shorter project schedule.

The purpose of Reliability Testing is to demonstrate that the shutdown system software meets its reliability target in producing a trip signal when demanded and no trip signal when not called for (Reference [1]). After being successfully tested by using the complete suite of Validation test scripts, the VTC will be used to produce the expected outputs for each set of random inputs applied to the PDC for Reliability Testing.

During the Reliability Testing of the shutdown system software, both the actual PDC and VTC receive the same set of random inputs. The actual PDC outputs are measured and compared with the VTC outputs. The test is considered successful when both outputs are consistent.

5. Virtual Display Computer

The Virtual Display Computer (VDC) shows, in graphical and numerical formats, the tester's expected results, the target computer and the VTC status such as tripped states and the analog setpoints. The tester can select different types of display, or turn off the VDC to speed up execution of the test scripts.

The VDC provides a convenient visual means during debugging by displaying expected and measured I/O values.

6. PDC Simulator

The PDC Simulator is an emulator of the actual PDC. It is actually composed of a VTC with I/O hardware cards. The function of the PDC Simulator is to allow extensive testing of ATLIN integrated with the NI hardware and the V&R test scripts, in advance of receipt of the actual PDC.

In addition, all V&R preparation work on the test procedures and test scripts can be advanced in the schedule using the PDC Simulator, to reduce the schedule risk by bringing forward the end date of this preparation work, prior to receipt of the PDC, target computer.

Updating the PDC Simulator to the latest PDC design is automatic once the VTC is updated. This avoids effort to update the PDC Simulator as the PDC design progresses.

The PDC Simulator can also be used for training V&R staff. When the actual PDC is available, the PDC Simulator is no longer required. Since the hardware components are identical to the V&R test rig, they become available as spares during V&R testing of actual PDC.

7. Progress of Preparation for V&R Testing

The V&R test rigs with the ATLIN software have been extensively tested using test rig test scripts especially designed for testing the rigs. In addition, all V&R test scripts for testing the PDC shutdown system software are run on the V&R test rigs using the PDC Simulator, before the actual PDC is available. The test results show that the new V&R test rigs meet the requirement for complete, accurate, and reliable V&R testing of the shutdown system software.

Before commencement of the formal V&R testing of the actual PDCs, the test rig I/O cards are calibrated and all ATLIN commands formally tested with a QA witness. The hardware making up the test rig is documented by serial numbers. In addition, all documentation on the test rig hardware and software will be issued, prior to the V&R test rig QA certified as ready and in a known configuration for the formal V&R testing of the PDC.

8. Conclusion

The redesigned V&R test rig with ATLIN, VTC, VDC, and the PDC Simulator provides a flexible, cost effective means to develop test scripts to perform V&R testing. More importantly, by using the V&R test rig, the V&R testing of the shutdown system software is fully documented and repeatable.

Long test sequences can be daisy chained to run un-attended on the rig, resulting in more efficient use of the tester's time. The automatic generation of test logs and reports reduces the effort and eliminates transcription errors in preparing the test report.

The ATLIN upgrade has maintained all functions in the previous version with additional features as a result of previous V&R testing experience feedback. In addition, it improves the accuracy of timing measurement to be better than 2ms.

9. Reference

[1] J. S. Baxter, A. Ranger, V. Lau, M. Chan, J. Ballyk and A. McDonald, "A CATHENA-Based Approach to the Development of Shutdown System Reliability Test Profiles", 28th Annual Conference of the Canadian Nuclear Society, 2007 June 3 to 6.