TRIALS, TRIBULATIONS, AND PITFALLS USING COMMERCIAL INSTRUMENTS FOR DATA ACQUISITION*

R.C. Lee#, R.H. Olsen, K.L. Unger, BNL, Upton, NY 11793, U.S.A.

Abstract

Brookhaven National Laboratory's Relativistic Heavy Ion Collider (RHIC) uses many commercially available instruments – for example spectrum analyzers, oscilloscopes, digital volt meters, signal generators - as integral parts of instrumentation and control systems. Typically these systems are remotely controlled. Using commercial instruments has many benefits. Manufactures have the skill, knowledge, and experience to produce high quality products. The price performance ratio is hard to duplicate. There are also disadvantages. Proprietary interfaces, single platform drivers, and reliable operation provide challenges for implementation and unattended operation. Several of the systems used at RHIC will be described. Their issues and solutions will be presented.

BACKGROUND

Some of the systems at RHIC and the injector accelerators of the Collider-Accelerator Department (C-AD) using commercial instruments for data acquisition and/or control are:

- Beam current monitor -- high precision digital voltmeter, current source.
- Beam profile monitors -- cameras.
- Polarimeter -- high voltage power supplies, multi-channel digital voltmeter.
- Pulsed power supplies -- oscilloscopes.
- Schottky cavities -- spectrum analyzer, oscillator.
- Stochastic cooling -- network and spectrum analyzers.
- Vacuum system -- ion gauge and ion pump controllers.
- Wall current monitor -- oscilloscopes.

When the accelerator is in operation these systems run unattended. Application programs control settings and acquire data. Much of the data acquired is logged for later analysis.

COMMERCIAL INSTRUMENTS

The focus here is on instruments designed primarily for bench-top applications. Instruments with front panel knobs and controls or virtual front panels as in plug-in units for PCs. In our applications these instruments are used remotely. For the most part without human intervention.

Why use them

Manufactures have invested a great deal of time and money producing instruments which perform their functions superbly. For instance an oscilloscope can provide the functionality to digitize many points of a high bandwidth signal over a wide range of input voltages.

These instruments also provide an important function for the user. Signals can be viewed and controls changed when the system is commissioned or during diagnostics.

It is important that instruments can be used both locally and remotely.

PROBLEMS

Reliable Operation

The systems using these instruments must always be in working order when the accelerator is in operation. It is necessary to be able to restart an instrument if it should malfunction. At RHIC we use either an in-house designed module, interfaced via a dedicated serial control link, or a commercially purchased module (WTI IPS series [1]), interfaced via Ethernet. The WTI has one command port for control of all channels (4, 8 or 16). Special attention must be taken when ports are allocated to several systems. As there can be only one command port open at a time each system must keep track of all port assignments. Status queries require parsing the response to select the port of interest.

Cyber Security

Many of these instruments are based on Microsoft Windows operating systems. This can be a big advantage -- using Remote Desktop allows access to all the features of the instruments. It is also a disadvantage. At BNL Windows PCs are required to be on a domain administered by the Information Technology Division (ITD), have a password locked screen saver, use BNL domain accounts, and several other requirements to enhance cyber security. Thus there is a conflict of interests -- use as a bench-top instrument and maintaining cyber security.

Types of Interfaces

Typically remote control is accomplished using one or several protocols such as:

- GPIB (IEEE 488)
- Serial (RS-232, RS-422)
- Ethernet (telnet, TCP/IP, HTTP)
- Firewire (IEEE 1394)

Each of these can present problems to be solved. GPIB and serial interfaces may require intermediate devices acting as bridges in order to allow Ethernet access to the instrument. Ethernet interfaces may have poorly implemented TCP stacks – network security scans, which

Industrial System in Exp./Acc. Physics controls

BACKING UP YOUR REGISTRY IS ALWAYS RECOMMENED IN THE EVENT THAT A MISTAKE IS MADE
HAVE AT LEAST ONE OTHER ACCOUNT WITH ADMINISTOR PRIVILIGES

These steps will force the specified program to be run instead of the normal windows shell..

1. From an account with administrative rights, create a new account and give it administrative rights as well.
2. Log off and onto the new account you just created (This account must have admin rights).
3. Open the registry editor by clicking Start – Run – and typing "regedit" in the space.
4. Locate the registry key
   HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
5. In the right pane – create a new string value and name it "Shell".
6. Change the value for the newly created string to the application executable you wish to solely run on this
   account including the path.
7. Close the registry editor.

To automatically log on this account, instead of being prompted for credentials, follow these steps.
1. Locate the registry key
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
2. In the right pane open the string value "AutoAdminLogon". If it doesn't exist – create it.
3. Change the value of "AutoAdminLogon" from "0" to "1".
4. In the same pane, add another string value called "DefaultUserName".
5. Change the value for "DefaultUserName" to the name of the account you created for limited access.
6. Add another string value called "DefaultPassword".
7. Change the value for "DefaultPassword" to the password you created for the limited account. If no password
   was set you can leave this blank.
8. Close the registry editor.

These last steps will disable the task manager so that no additional programs can be run or closed.
1. Click Start – Run – and type "gpedit.msc" in the space.
2. In the left pane expand the key called "User Configuration".
3. Under "User Configuration" expand "Administrative Templates".
4. Under "Administrative Templates" expand "System".
5. Under "System" open the folder called "Ctrl+Alt+Del Options.
6. Double click "Remove Task Manager" and change the setting from "Not Configured" to "Enabled".
7. Close the policy editor.

The newly created account will now run only the specified application with no other control to the computer until
logged off and back on as a different user.

***NOTE – These actions were performed only on a Windows XP machine. They will most likely work on
Windows 2000 or Vista as well but may require some minor changes.***

Figure 1: Kiosk Mode - Creating a limited account for access to only one specified application [2].

are periodically conducted by ITD, may hang the device or the device may adversely impact the Ethernet.

Software/Drivers

Manufactures can also make our jobs difficult. Interface protocols may change from one model of an instrument to another. Sometimes drivers/applications are not available for the version of the operating system on which the instrument is going to be used.

One area of development at RHIC involves the use of IIDC/DCAM cameras for beam display and analysis.[3] This project makes use of open source software called libdc1394.[4] It is used for communicating with cameras which implement the DCAM protocol on computers running the Linux operating system. Having this library available was a great asset to software development, but

we ran into several roadblocks along the way, and it meant making several changes to the way we typically develop code. For example, on more than one occasion the open source team made the decision to substantially change the applications programming interface (API), while also introducing some attractive new capabilities; in order to get the new features we needed to make some major changes to our code. They also used a system for version control which isn't compatible with the system we use. Not too long ago we reached a point where the features already available address our needs pretty well, so we have stopped updating the library, even though the open source development continues.
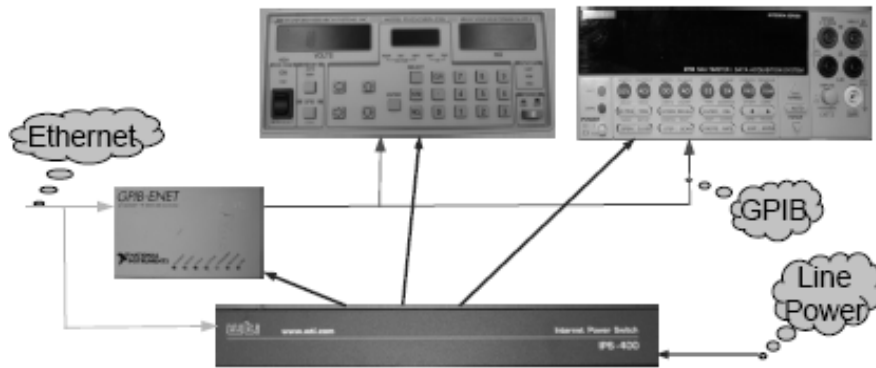
Industrial System in Exp./Acc. Physics controls

Figure 2: Remote Power Reset.

SOLUTIONS

Cyber Security

The steps in Figure 1 outline three areas to modify to implement kiosk mode – create a local-domain user restricted to run one program, enable automatic logon, and remove access to the Task Manager via Ctrl-Alt-Del. In this mode the instrument performs as a bench-top device -- controls and displays are available and the instrument can be rebooted without user intervention.

Users can still logon, either locally or remotely, to the ITD domain to perform maintenance tasks -- Windows updates, instrument updates, virus scans, or transfer files. In this mode the instrument is being used as a desk-top PC and can be monitored for security violations.

Reliable Operation

Remote power switches (Figure 2) are essential to be able to restore operation if an instrument or interface device, such as an Ethernet-GPIB controller, malfunctions. This cannot be emphasized enough. At RHIC and its associated accelerators we continue to add remote power switches to existing systems to facilitate recovery from a malfunctioning instrument.

REFERENCES

[1] Western Telematic Inc., http://www.wti.com.
[2] Ryan Golinski, BNL, personal correspondence.
[3] R.H. Olsen, D. Gassner, L.T. Hoff, "Using an IIDC/DCAM camera for beam display and analysis", ICALEPCS (2009).
[4] Damien Douxchamps, Libdc1394: The API for IEEE1394/ Firewire cameras, http://damien.douxchamps.net/ ieee1394/ libdc1394.

Industrial System in Exp./Acc. Physics controls