# REMOTE CONTROL OF THE ATLAS SUPERCONDUCTING ACCELERATOR*

F. H. Munson, R. C. Pardo, M. A. Power, R. C. Raffenetti, R. J. Carrier**
*ANL, Argonne, IL 60439, USA*

## ABSTRACT

The ATLAS (Argonne Tandem Linear Accelerator System) control system has always provided remote access. In the distant past this access was limited to a telephone modem (modulator – demodulator), and it was used primarily to resolve software problems using a character based terminal. More recently, however, with the arrival of the Internet and newer technologies complete remote control and monitoring of the accelerator using GUIs (Graphical User Interfaces) has been realized. The communication speed of the remote connection is limited primarily by the remote user's network interface. Except for this limitation access is complete and flexible, and allows for full control of the accelerator from anywhere in the world. Remote access to an accelerator's control system is not a new idea, but variants of the same idea are probably being used at different installations. This paper describes the approach taken to remote control and monitoring of ATLAS.

## INTRODUCTION

Focusing primarily on nuclear physics, ATLAS is a hybrid heavy ion accelerating system consisting of a Tandem electrostatic accelerator and a superconducting LINAC (Linear Accelerator). The system is capable of accelerating low-energy heavy-ion beams of isotopes ranging from hydrogen to uranium to nearly 20% the speed of light.

ATLAS operates 5.5 to 7 days a week, 24 hours a day with a total staff of only 19 persons. The operations crew totals 7 persons. The result is that many evening, midnight, and weekend shifts are staffed with only one operator, and no other support staff is on site. Thus when problems develop, system experts must either fix the problem over the telephone or come to the Laboratory. Remote access to the control system provides a third option for diagnosis and even repair depending on the problem.

Remote access to the ATLAS control system has been used for many years by the controls group to monitor the control system, and to fix problems that develop after work hours. Recently, full access to all features of the control system has been implemented. This allows system experts for various subsystems of the accelerator to log on from home or their hotel room and monitor the facility operation and correct problems that arise. This has been useful on occasion in monitoring and tuning ion sources for ATLAS.

This paper describes the current state of remote access, and discusses how the system may be developed further to enhance the ability to have full control of the accelerator from the internet.

## THE CONTROL SYSTEM

The foundation of the ATLAS control system currently consists of a server computer and two primary subsystems. The first of these subsystems is a single CAMAC (Computer Automated Measurement And Control) Serial Highway, which links as many as 18 CAMAC crates. The second subsystem is an Ethernet based LAN (Local Area Network).

The real-time software aspects of the control system are handled by Vista Control Systems' software package "Vsystem" [1]. Vsystem is a network distributed control system software that provides distributed database access. The package includes a library of callable database access routines, several database access utilities, and a GUI display process. At ATLAS, Vsystem runs on the HP OpenVMS [2], Microsoft Windows [3], and Linux [4] operating system platforms.

* This work is supported by the U.S. Department of Energy, Nuclear Physics Division, under contract W-31-109-Eng-38.
** Undergraduate Research Participant

## REMOTE ACCESS

The ATLAS control system LAN is isolated from the outside world. However, a system that provides both VPN (Virtual Private Network) and NAT (Network Address Translation) capability provides secure authenticated remote connections to the otherwise isolated control system.

### *Motivation and Goals*

Prior to implementation of the VPN, access to the isolated network from outside the ATLAS facility was provided by a "dial-up" modem, and access from within the facility was provided by workstations with two network connections. These "bridge" PCs gave local access to the control system LAN, while providing an indirect avenue to software and patches obtained by external download. While the PCs provided no routing function, the arrangement violated the developing security policy of the Laboratory. Moreover, there was no remote access except for the dial-up modem, and modem use at the Laboratory is now being discouraged.

Therefore, the goals of implementing the VPN were to maintain independence, improve security, and allow highly regulated remote access to the control system LAN from the outside for administrative purposes. The latter was not expected to be a high demand need, and the preferred access method would be a familiar one not requiring new tools or complex procedures. The common remote computer was a PC with some version of Microsoft Windows, either in the Internet environment, or just not within the isolated ATLAS LAN.

### *VPN Server Configuration*

While the laboratory-provided VPN permitted remote computers to securely access Laboratory resources, it could not satisfy the need for access to the isolated ATLAS LAN. After investigating VPN alternatives, it was determined that Microsoft Windows 2000 Server running on a PC with two network connections was a cost-effective solution that met all of the goals. The VPN satisfied the isolation and security requirements, while the software supported the remote client platforms. Other commercial VPN solutions were targeted to high-bandwidth requirements, and typically had material costs two or more times that of the present solution.

Figure 1 is a schematic of the remote access arrangement. The basic elements include a PC external to the ATLAS LAN (the remote or home PC), the Internet, the Laboratory firewall, and the isolated LAN in which the control system computers participate. The isolated LAN includes a standalone Active Directory "forest" that provides authentication and other services for the Windows computers. There are two domain controllers, and each controller runs DNS (Domain Name Service). The RRAS (Routing and Remote Access Server) is a member of the domain, and clients that access the LAN through its VPN function, authenticate to the domain. No access to the isolated LAN from the outside is permitted without authentication.

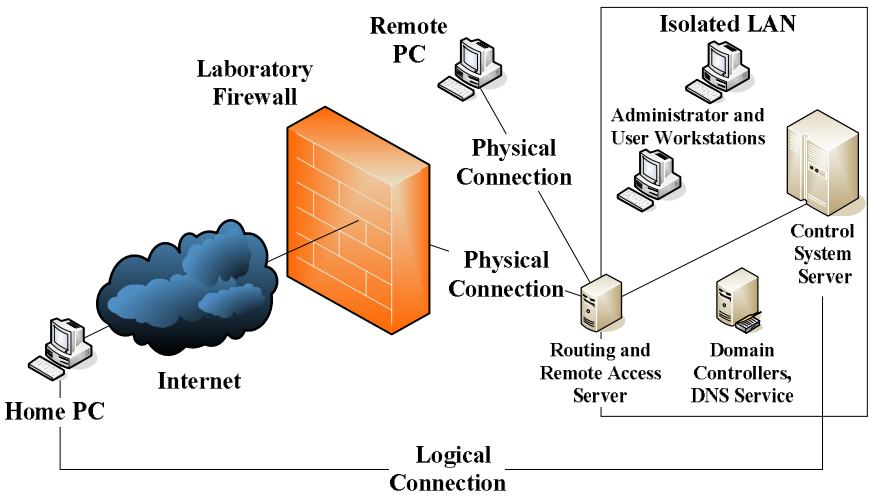


Figure 1: Remote Access Arrangement

An authenticated VPN connection from an external PC to a computer inside the ATLAS LAN creates a logical, end-to-end encrypted connection, in which the external PC acts as a member of the ATLAS LAN. The RRAS server has a pool of ATLAS LAN IP (Internet Protocol) addresses that it assigns to external PCs. All logical connections consist of physical connections through the RRAS server from inside or outside of the Laboratory firewall.

### *VPN Client Configuration*

The CMAK (Connection Manager Administrator Kit) wizard is a tool that guides "service profile" creation. The service profile assigns all of the settings for users. The result is a single-diskette installation kit that is customized for the ATLAS VPN and its environment. The user simply executes a single file on the diskette to install the VPN client software on his or her remote computer system.

### *NAT Configuration*

In addition to the VPN function, the RRAS server allows computers inside the isolated LAN to access the outside world via a NAT function. This latter feature permits the direct download of software and patches from the Internet. The NAT configuration enables users of computer systems, physically connected to the isolated ATLAS LAN, to participate in the environment outside of the ATLAS LAN just as if they had a direct connection to the Internet. When using the NAT there is no access to the isolated ATLAS LAN from the outside, unless first solicited from a system within the isolated LAN.

### *Remote Desktop Access*

At the outset of this project the initial goal was to provide convenient remote access to control system computers for administrative functions. While successfully establishing a VPN connection to the control system LAN is a major step in providing secure remote access, it does little to provide the remote user with an interface to the control system's computers.

An interface to the control system's OpenVMS systems, to perform administrative functions, is easily established by using terminal emulation software operating on the remote user's PC. Connections can be made to these OpenVMS systems using a remote access tool such as "telnet".

However, the preferred method at ATLAS for establishing remote access to the control system's Microsoft Windows computers for administrative purposes is through the use of RDP (Remote Desktop Protocol). After establishing RDP sessions with Microsoft Windows systems, such as the domain controllers described previously, the external user can use the same tools remotely that administrators use while working directly on those systems. This has the advantage of freeing the staff from licensing and maintaining the same tools on the external PCs.

## USER INTERFACE OPTIONS

As discussed previously, providing remote access is only part of what is necessary to give the remote user complete and convenient access to a control system. Character based terminals are among the first devices used to provide a remote user with an interface to a computer system. Today, most computer user interfaces rely on a "windowing" system of some sort, and these systems incorporate character based terminals as just another window. These "virtual terminals" are used, as in the past, primarily for command line operations. Arguably, the two most prevalent windowing systems in use today are Microsoft Windows and the X Window System [5], which is often referred to as simply X Windows. Vsystem's display process is a graphical user interface that has been designed to run in both the Microsoft Windows and X Windows environments providing both as an option.

### *X Windows Option*

The X Windows option requires that the remote user's computer has an X Windows "server" process running. An X Windows "client" process, such as an X Terminal, is then started on a local control system computer, but the X Terminal display is sent to the user's remote computer. Using the X Terminal the user logs into a control system computer and starts the Vsystem display utility. The Vsystem display utility runs as a process on a local control system computer performing local database access, but the actual display is sent back to the remote user's computer using X Windows commands. Most of the traffic over the network connection is X Windows traffic. This option, shown in Figure 2, is more generic and can be adopted by a variety of control system software. The primary advantage to this option is that the local control system displays and software can be updated without having to propagate those changes to the remote systems.

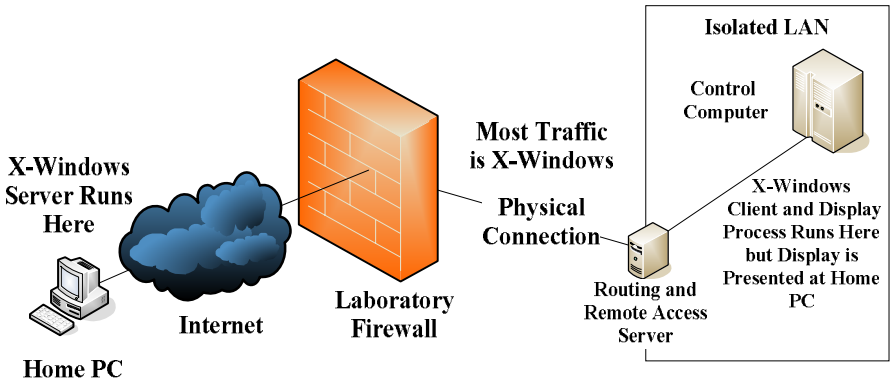


Figure 2: X Windows Remote Access Option

### *Vsystem Option*

In order to use this option Vsystem software would have to be installed on the remote user's computer, which could be running an assortment of different operating systems. With this configuration the Vsystem display utility runs on the remote user's computer instead of a local control system computer. Database access is performed on behalf of the remote display process by a local database access process on a local control system computer. The connection between the database and the remote Vsystem display process is accomplished using Vsystem networking software. Most of the traffic over the network connection is Vsystem traffic. The Vsystem option is useful if the goal is to decrease the use of local control system computing resources. This option is shown in Figure 3. It is not currently used routinely at ATLAS, because the X Windows option is easier to implement and maintain on the remote user's computer. The Vsystem software would need to be licensed and installed on each remote computer and updated as changes occur on the local control system.

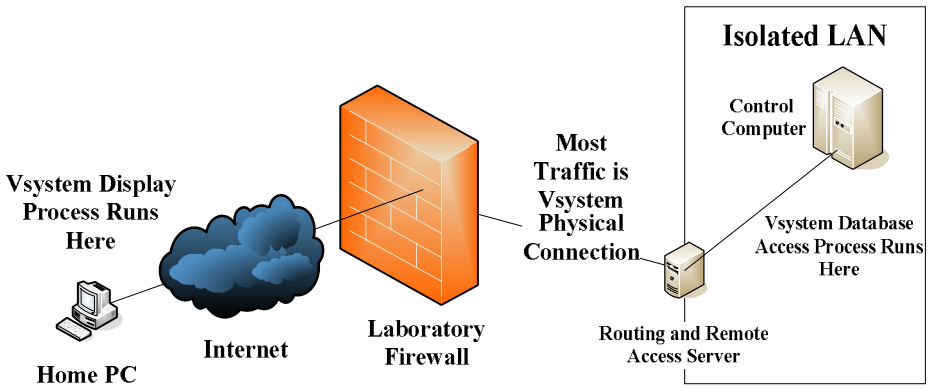


Figure 3: Vsystem Remote Access Option

## PERFORMANCE ISSUES

The X Windows option has been installed for use on some staff computers, both office and laptops. This option has been used to both monitor accelerator operation, and to actually control certain aspects of the accelerator remotely. So far this feature has been used only in developmental activities and in trouble shooting situations. Actual remote control of the beam, delivered for research, has not been attempted at this point.

Performance of the remote interface has been excellent when used in conjunction with a DSL (Digital Subscriber Line) or Broadband connection. Significant ion source development activity has been accomplished from a home computer by at least one of the authors. This has been possible because beam current monitoring has been fully implemented through the computer system for local ion source Faraday Cups, but has not been fully implemented in the rest of the facility. Thus it is possible to tune nearly all aspects of the ion source and nearby beam analysis and transport systems through the control system. Under these conditions, an occasional break in the communications has been experienced, which usually lasts for only a few seconds. Otherwise, information update speeds are quite adequate to give the remote operator the feel of real-time control.

## CONCLUSION

The in-house assembled and configured VPN/NAT system along with the X Windows Remote Access option has proven to be a low cost - low maintenance system. To further increase its usefulness we are working toward implementing additional beam diagnostics information fully into the computer system, thus allowing beam control and tuning of any aspect of the accelerator over the Internet.

## REFERENCES

[1] Vista Control Systems, Inc., Los Alamos, NM, USA.
[2] Hewlett-Packard Corporation, Palo Alto, CA, USA.
[3] Microsoft Corporation, Redmond, WA, USA.
[4] Linux, A registered trademark of Linus Torvalds.
[5] "X Windowing System", A system resulting from a collaborative effort of a consortium of vendors and the Massachusetts Institute of Technology.