UCRL-JC-143539

Designing Remote Monitoring Systems For Long Term Maintenance And Reliability

G. E. Davis
G. L. Johnson
F. D. Schrader
M. A. Stone
E. F. Wilson

This article was submitted to Symposium on International Safeguards: Verification and Nuclear Material Security
Vienna, Austria
October 29 - November 1, 2001

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

April 11, 2001

Designing Remote Monitoring Systems For Long Term Maintenance And Reliability

G. E. Davis
G.L. Johnson
F. D. Schrader
M. A. Stone
E. F. Wilson

April 11, 2001

As part of the effort to modernize safeguards equipment, the IAEA is continuing to acquire and install equipment for upgrading obsolete surveillance systems with digital technology; and providing remote-monitoring capabilities where and when economically justified. Remote monitoring is expected to reduce inspection effort, particularly at storage facilities and reactor sites. Remote monitoring technology will not only involve surveillance, but will also include seals, sensors, and other unattended measurement equipment.

LLNL's experience with the Argus Security System offers lessons for the design, deployment, and maintenance of remote monitoring systems. Argus is an integrated security system for protection of high-consequence U.S. Government assets, including nuclear materials. Argus provides secure transmission of sensor data, administrative data, and video information to support intrusion detection and access control functions. LLNL developed and deployed the Argus system on its own site in 1988. Since that time LLNL has installed, maintained, and upgraded Argus systems at several Department of Energy and Department of Defense sites in the US as well as at the original LLNL site. Argus has provided high levels of reliability and integrity, as well as reducing overall lifecycle cost through incremental improvements to hardware and software. This philosophy permits expansion of functional capability, hardware upgrade and software upgrade without system outages and with minimum outage of local functions.

This presentation will describe Argus design strategies and lessons learned from the Argus program as they apply to the design, development, and maintenance of a remote monitoring network.

Hardware failures, software failures, and communication outages are expected and must be addressed by astute selection of system architecture. A combination of redundancy, diversity, and effective functional allocation between field and system level components should allow the system to tolerate component failures and communication interruptions. To the extent practical, field functions should continue to operate given communications interruptions or failure of central computers. Complete system functionality and history must be restored quickly after communications or central computer functions are restored. The needs for redundant functions to tolerate hardware failure and diverse functions to tolerate common cause (e.g., software errors) failures should be carefully evaluated and addressed in the system design.

Fundamental changes to communications backbone are expensive. Careful initial design of this feature is important to minimize the cost and system upset of future upgrades. The design should incorporate performance margin to support future functional enhancements and support open communications protocols that allow new types of equipment to be added to the system without significant changes.

Any long-lived system will continually evolve. Therefore, hardware and software design must provide enhancement of capabilities and backward compatibility. Consideration of future system directions in design allows the system to evolve gracefully over time. Doing this requires a good understanding of customer needs and wishes feeding and a strategic plan for system evolution. With this approach, significant enhancements in functionality and migration away from obsolete equipment can happen with out the need for major system outages.

Upgrade of field units must be fast, simple, and secure. Storage of field software as firmware provides a high level of software security and allows "drop-in" software upgrade.

Argus software was designed with ease of modification and upgrade in mind. The product uses Ada for most of the software, taking advantage of its packaging and exception handling capability for effective organization of the software. Recent software has been developed using C++ and object-oriented design techniques to improve maintainability.

Secure communications does not necessarily require secure communications systems. Encryption and tamper detection features can assure a high level of data integrity over non-secure communications system. Security features must be readily upgradable to allow improvement as the threats and the defenses become more sophisticated. A combination of hardware and software features can assure a high level of data integrity while supporting frequent enhancement.

The overall Argus system continues to support the capability for incremental modernization without complete system replacement since its initial installation in 1988. Several sites have upgraded host computers, field processors, console computers and other significant system components. The system software is now in its 22nd major release, with new functionality included with each release. Argus continues to be a robust security system, and the development team continues work on further modernization of software and system components.

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.