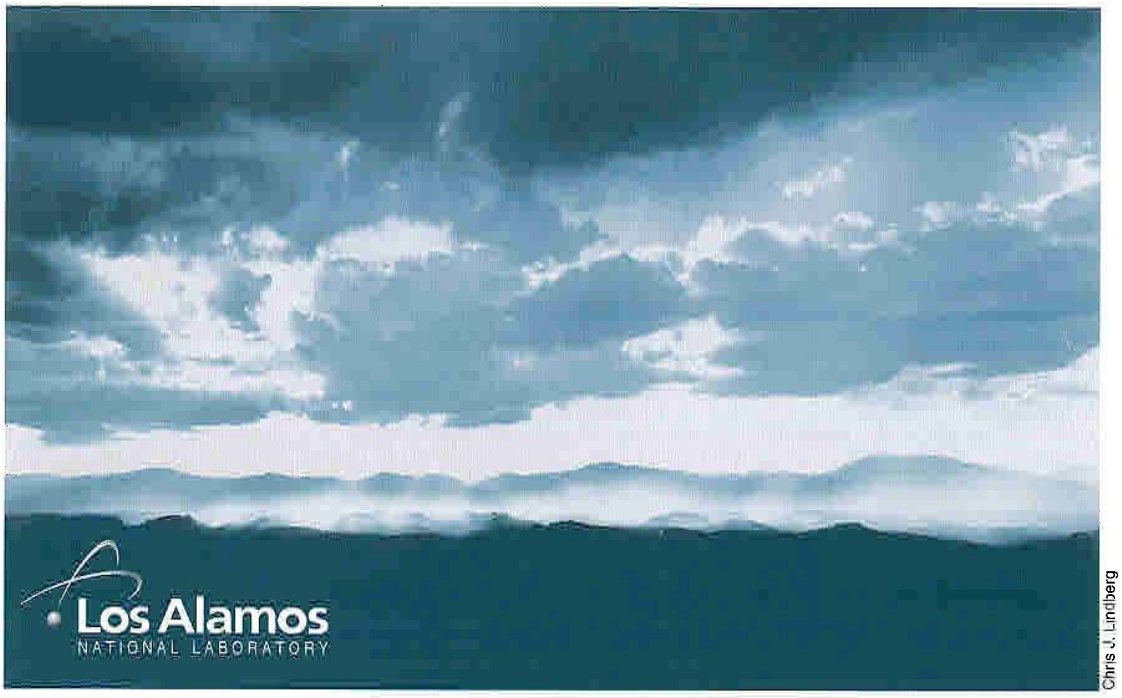
LA-UR-04-4448

Free Topology Networks and Their Application in IAEA Safeguards

Rohun Gholkar, student, Rensselaer Polytechnic Institute
Summer Student, Los Alamos National Laboratory (summer 2004)
Safeguards Intern at IAEA (June 2003 – January 2004)

James K. Halbig, Los Alamos National Laboratory
United States Cost Free Expert at IAEA
Los Alamos National Laboratory
Safeguards Science and Technology Group (N-1), MS E540
Los Alamos, NM 87545

Presented at the
Institute of Nuclear Material Management
45th Annual Meeting
Orlando, Florida
July 18-22, 2004



This is a preprint of a paper intended for publication in a journal or proceedings. Because changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

Free Topology Networks and Their Application in IAEA Safeguards

Rohun Gholkar, student, Rensselaer Polytechnic Institute
Summer Student, Los Alamos National Laboratory (summer 2004)
Safeguards Intern at IAEA (June 2003 – January 2004)

James K. Halbig, Los Alamos National Laboratory
United States Cost Free Expert at IAEA

Los Alamos National Laboratory
Safeguards Science and Technology Group (N-1), MS E540
Los Alamos, NM 87545

Abstract:

IAEA Safeguards systems must perform in challenging environments with many varied operational constraints. The ability to dynamically interconnect instruments and inspector interfaces without being thwarted by the transfer medium or physical configuration of a network is of paramount importance when implementing integrated safeguards systems. A free network topology provides the robust set of options useful to the IAEA for successful connection of common instruments and collection devices in different facilities with varying physical layout. A general set of requirements for integrated safeguards systems networks is discussed, and an example of a current implementation is given. Areas of focus include authentication/encryption, bandwidth requirements, and possible technologies that can be used to maximize the versatility of free topology networks for safeguards systems.

Introduction

Today, nuclear safeguards are being applied in a growing number of facilities throughout the world. As a result, inspection agencies such as the International Atomic Energy Agency (IAEA) increasingly rely on unattended, intelligent, autonomous instruments to supplement the capabilities of a limited number of safeguards inspectors. The effectiveness of the inspectorate is extended across facilities while the inspectors are absent, and the impact of safeguards inspections upon facility operations is reduced.

The benefits of unattended monitoring instruments are enhanced by the use of computer networks. Networks provide a means to securely[1] move monitoring data to a central collect computer and for instruments to trigger each other into entering a higher state of awareness. An instrument that detects a significant activity (a change in radiation level) can send a signal to another intelligence, such as a camera, to take supplementary action—in this case, taking pictures to show what is causing the change in radiation. Inspectors can then efficiently retrieve the data from multiple instruments from a single networked collect computer, allowing them to spend less time in the facility and reduce their radiation exposure. Because the inspector spends less time at a facility, travel expenditures are lowered for the inspecting agency, and there is a facility-welcomed reduction in the time that an operator must provide in-facility support.

Remote access to safeguards information provided by networking technology can be used to move inspections data to a remote location without the need for an inspector to travel to the facility for data retrieval, reducing visits and thereby further reducing travel costs. There are, however, facility security and general political problems associated with the remote transfer of safeguards information across national boundaries. As a result, this capability is not currently in wide use. This same technology is also used to transport state-of-health data from instruments in a facility to headquarters or a regional office. Such capability allows an inspection agency to quickly diagnose and then manage inevitable failures that rarely, but certainly can occur. This gives regulatory bodies the ability to be cognizant of the operating conditions and/or performance of their systems on a regular basis, without an intrusive on-site visit. Clearly, both regulatory agents as well as facilities welcome any reduction in the number of maintenance-related trips whose sole results are the verification of a system's operation. These capabilities are being exploited by the IAEA regularly in newer safeguards installations and in upgrades to older ones.

Network Topologies

Networks are a collection of devices electronically linked together for the purposes of data transfer and/or communications. The structure of these links is referred to as a network's topology. Figure 1 graphically illustrates common topologies found in computer networks. The star and tree (collection of stars), is commonly used for Ethernet networks, while free topology LON[2]-based networks can be configured as a hybrid of any topologies.

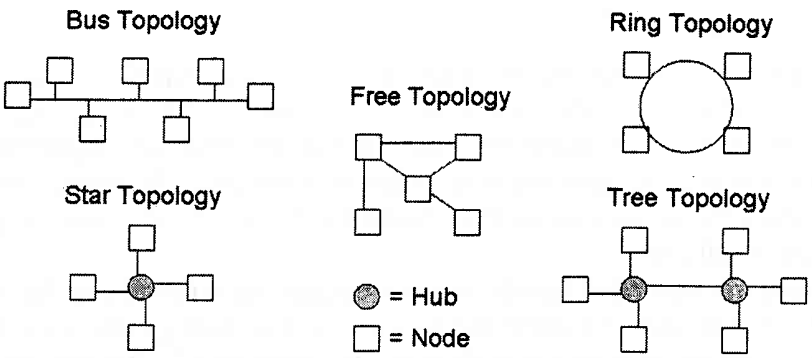


Figure 1, Graphical Representation of Network Topologies

Requirements of Safeguards Systems Networks

The IAEA has been using unattended monitoring safeguards systems for over 15 years. These systems allow for continuity of knowledge with regards to the operation of a facility to be maintained during the absence of an inspector. Within certain limitations, the majority of UNARM (Unattended and Remote Monitoring) instruments used by IAEA are operated in an autonomous fashion. Thus, an UNARM system operates autonomously for the majority of an inspection period, and an inspector then travels to a facility to retrieve previously collected data from each instrument or camera's enclosure, allowing him/her to review the operational signatures of the facility and determine if they are consistent with safeguards declarations. The appropriate use of network technology can further streamline safeguards inspections by allowing data to be automatically collected and centralized in one location for later, and possibly remote, retrieval. Time is conserved because an inspector only visits one location within the facility to obtain data. This location is often in a computer room far from radioactive areas, and as a result, the use of a network contributes to reduced radiation exposure for the inspector.

Although the requirements of safeguards systems networks are evolving, certain areas of concern remain constant, such as: bandwidth requirements, data authentication/encryption, size and power consumption, the necessity for easily distributable nodes, and flexibility of network media. Average data rates for typical radiation-based instruments are low due to the small number of bytes per data acquisition. The maximum data rate in a typical radiation monitoring application is about 50 bytes/sec. Generated data can range to several orders of magnitude less, depending on the data acquisition rate, the type of data being saved, and the conditions under which they were saved (i.e. data filtering[3]). When supplementary video images are also being transferred, as is the case in integrated safeguards, the average bandwidth requirements can rise significantly. A typical video frame may produce 15000 bytes of information. Based on the safeguards application and the amount of data being generated (radiation data, still images, real time video, etc.), an appropriate technology should be selected. Table 1 lists some possible *average* data generation rates, however, significantly higher video data generation rates are possible under some facility operation conditions.

For integrated safeguards, a higher bandwidth network is generally added between video servers, collect stations, and review stations due to the number of bytes per transmitted video frame and the number frames transferred. Video data on a small scale (handful of cameras), could be handled by a LON network. However, the network would operate fairly close to peak bandwidth

(78Kbits/sec), leaving little room to add more cameras or radiation detectors. Consequently, other technologies (i.e. Ethernet with a bandwidth of 100Mbits/sec) are used to carry the increased load.

It is difficult, expensive, and in many cases very intrusive to provide a secure media interconnection among network nodes in a facility—especially in retrofitted applications. Therefore, authentication[4] is applied to all transmissions moving in and out of the network nodes, including commands, controls, and data. Authentication of command and control messages prevents a potential adversary from being able to introduce "pirate commands" to an instrument over the network. Some people have proposed that encryption should be used to prevent people from learning about various system parameters or thresholds by watching traffic on the network--e.g. camera triggers. The argument can be made that if the security of a system requires keeping such information from the operator of the facility, then perhaps the system was not properly engineered and is inherently less secure than is required. That said, it is certainly possible to use components that add a layer of encryption to transmitted data on the instrument network, should a significant need arise.

	Radiation	Video	
Bytes/Transfer Unit (typical)	38	15,000	Bytes/sec
Unit Period (typical)	2	300	Seconds
Typical Bandwidth Per Acquisition	19	50	Bytes/sec
Filter or Trigger Conditions	Filtered to 2%, 80% of time	40 Triggers, 18 frames/trigger 10s heartbeat, 30s post period	
Filter or Triggered Bandwidth (Event-Average)	3.4	1,380	Bytes/sec
Not Filtered, Not Triggered Bandwidth (Daily Average)	20.2	50	Bytes/sec
Filter and Triggered Bandwidth (Daily Average)	3.4	176	Bytes/sec
Filtered and Triggered Daily Storage	1.74MB	15.2MB	Per Day

Table 1, Data Movement Rates/Instrument Type

In safeguards systems both data and command and control traffic must be secure. Transparent instrument channel authentication is desired to simultaneously protect the command and data traffic. Considering the size of command and data packets, where messages of a few 10s of bytes are repeated many times per minute, having the *instrument* apply a long authentication signature (128 bytes or so) to each packet becomes a wasteful use of resources. By authenticating all transmissions at the network nodes, everything sent on the network from node-to-node will be secure. The transparency of this layer means any intelligence using the network need not perform its own authentication/encryption. As a result, safeguards technologists are free to select instruments that require less processing power, increasing the cost effectiveness of the overall system. In a typical IAEA unattended integrated monitoring system, a network node is typically located at every distributed intelligence location (camera, detector enclosure, collect computer or other data-generating/-recording device). Often these nodes are not physically located near one

another. In this case, distance limitations of a particular network technology and/or media must be considered along with the possibilities and costs of implementing the network. For example, a typical Ethernet link[5] has a maximum distance of 328ft (100m) over unshielded twisted pair cabling, whereas a LON network connection, utilized by the IAEA in many UNARM systems, can operate at a maximum distance of 1,640ft (500m) over standard twisted pair in a free topology configuration.

Most safeguarded facilities were designed and/or built without forethought to having safeguards installed at the facility. In these cases, running any type of network cabling may be a physical problem and a costly undertaking. It has been noted that running new cables or having to use existing cables at a facility can quite often be an issue. As a result, the cabling scheme with the least stringent requirements is a practical solution. Although current IAEA installations of free topology networks typically involve copper wire media, it is not necessary for the wire used to meet more stringent CAT 5 cabling requirements of Ethernet. In fact, the LON-based networks used by IAEA can use the same wires to carry both the supply power for the network node as well as the network communications. This kind of flexibility comes in especially handy when implementing safeguards in an older facility, where existing cables are run through restricted penetrations in thick concrete walls, and running new cables would be quite costly.

A Current Approach to Safeguards Networks

A current example of free topology networking implemented in IAEA safeguards is the unattended integrated monitoring system at the BN350 breeder reactor facility in Aktau, Kazakhstan. At this facility, a combination of neutron detectors, gamma detectors, and video cameras is used to produce an integrated safeguards solution. A LON-based free topology network is used to transmit radiation data from instruments back to a set of redundant collect computers and for the same instruments to trigger individual video cameras located at strategic locations within the facility. The video data itself travels through a separate cabling system to a video server that in turn relays video images regularly to the RAID[6] storage system at the redundant central collect computers via a high bandwidth Ethernet connection. State-of-health data are moved over a virtual private network (VPN) away from this centralized storage area to a facility-remote SOH computer that transmits SOH statistics to headquarters when remotely requested or on a regular interval.

The network layout implemented has all of the instruments, cameras, and computers involved behind a physical layer of security, which we'll refer to as a "secure boundary." All data transfer within this boundary is considered physically secured (locked room or enclosure) and does not require any authentication or encryption. Channel authentication ensures that transmissions between boundary areas maintain data integrity without physically securing the cabling itself. Figure 2 illustrates this concept.

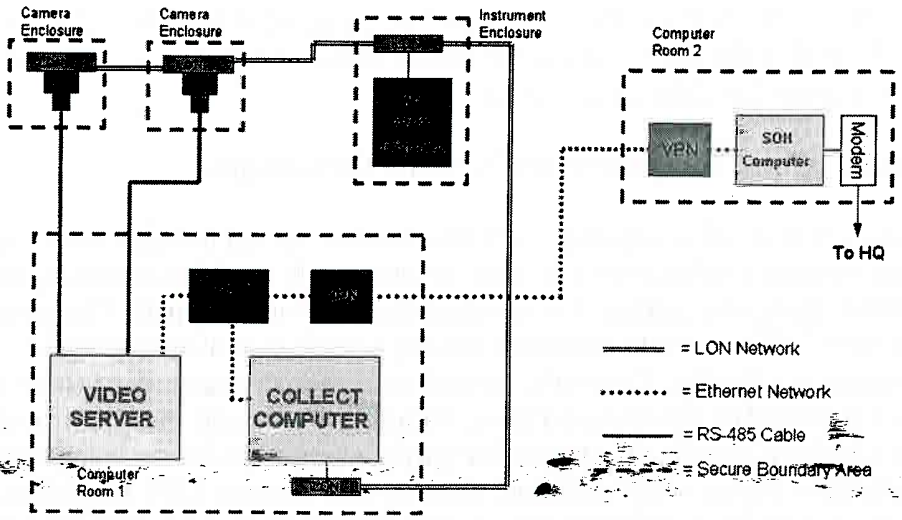


Figure 2, Secure Boundaries of a Safeguards Network

Free topology networking offers several advantages in this facility. The network topology in this installation, shown conceptually in Figure 3, generally resembles a ring. This adds reliability to the system because the network must be broken in more than one location to lose network communications. The distance between network nodes is often quite large and spans over multiple rooms. Large link distance limit for LON technology and its free topology characteristics drastically reduce wiring and installation costs. Having a long link distance eliminates the need for repeaters or extra hubs, and free topology lowers installation costs.

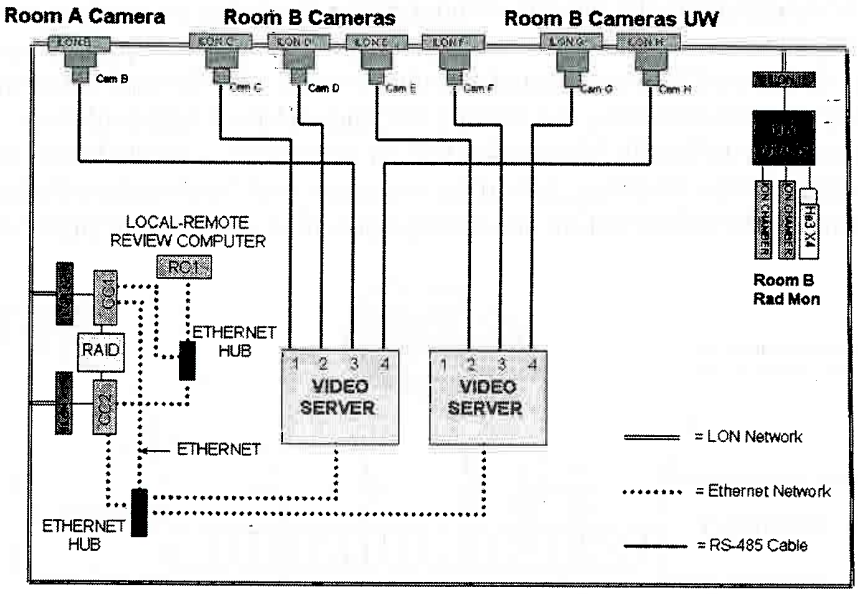


Figure 3, A Past Network Layout at the BN-350 Reactor Facility

The BN-350 is also a good example of when Ethernet and free topology technologies are appropriately combined to meet system requirements. Transferring the massive amount of video data being generated by the cameras in the facility would easily swamp a LON network operating in

the free topology mode. Fortunately, the system was designed to have the video servers conveniently located in the same room as the central collect computers, making Ethernet a localized cost-effective solution for video data transfer.

Potential Application of Complimentary Network Technologies

In some instances, free topology LON based networks can be made more versatile for safeguards use through combination with other commercially available technologies, such as radio frequency (RF) transceivers and media converters (i.e. LON-to-Ethernet). One such application might be when the IAEA wants to monitor a moving container of nuclear material, such as a railcar, between buildings at a facility. Currently, an enclosure with an unattended instrument and/or camera would be placed on the container along with a network node and GPS antenna. As a container travels along its path, the unattended system monitors radiation levels and triggers a camera to take video frames while recording position data from the GPS subsystem. Any time the container docks at a building, radiation data, position information, and video frames are transferred through a wired network link to a collect server for storage.

A potential alternate implementation, Figure 4, would be to have cameras mounted at various positions along the railway. As the car is traveling, it triggers not only its own camera, but also the strategically placed cameras near it, to take frames showing what is happening around the car (i.e. diversion of materials or terrorist attack). This could provide a significant advantage over the previous technique when trying to understand events surrounding a materials diversion. Now instead of one camera mounted on the railcar aiming directly ahead and capturing little to no view of a potential diverter, a multitude of images from various angles can be used to learn more about the diverters and the methods they may have used. Autonomous camera systems are mounted in self-contained enclosures along the railway without cables for power or communications. Both the car and camera enclosures contain their own independent mains power supply provided by a deep-cycle battery and maintained by a solar panel charging system. An RF-enabled network node is positioned at every camera enclosure, the moving car, and on top of both buildings. Radiation monitoring data and state-of-health information will be continually collected from the car without waiting for it to dock inside a building, providing inspectors with knowledge of actual radiological conditions surrounding the railcar before and during a potential diversion of materials.

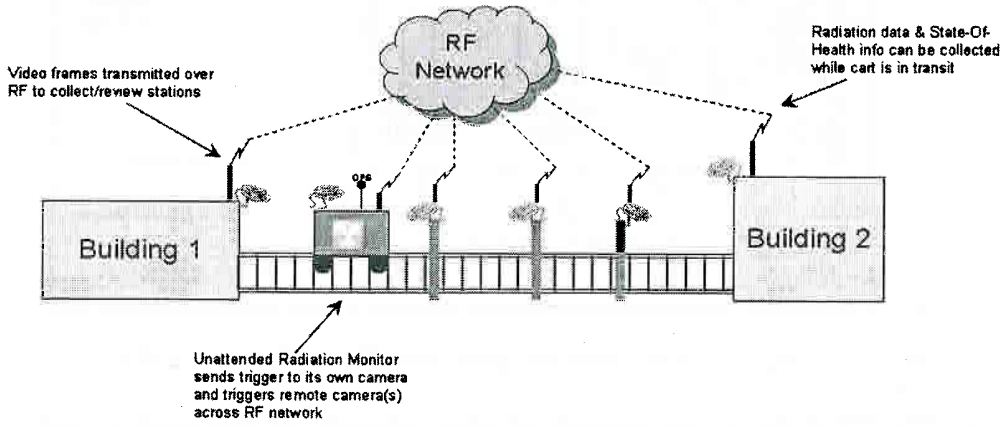


Figure 4, Potential Application of RF Technology for Moving Container Safeguards

The wireless network hardware could be implemented either as a direct LON-RF link or by first using a LON-to-Ethernet converter as an intermediate step, feeding a more powerful Ethernet-RF link. This decision is made based upon factors such as the number of devices on the network and physical distance between the buildings. Off-the-shelf RF transceivers for Ethernet are more prevalent and powerful than their LON-based counterparts and offer a larger suite of features such as built-in hardware encryption and remote network management.

Another interesting scenario might be when the maximum distance between two sides of a facility is so large that the standard copper wire media used by free topology LON networks can't be used. In this case, the IAEA would have two options: placing repeater nodes along a cable to enable the usage of copper-wire media or using LON-to-Optical Fiber media converters. Using repeaters could potentially be expensive, given the cost of additional network nodes and the difficulty of delivering power to their location. However, if the facility is an older one and already has copper media running through it, the cost of repeaters could offset the potential price of running brand-new optical fiber. Commercially available, off-the-shelf optical conversion modules are a cost-effective way to handle distances of up to 2 km and materials costs are kept to two converters and the optical fiber itself, which has become less costly in recent years. Thus, this is an attractive and relatively inexpensive option for newer facilities that have fewer potential problems associated with laying new cables.

Summary

The important business of implementing international nuclear safeguards is a challenging and costly endeavor. The cost of implementing and using integrated safeguards systems can be reduced through the efficient use of a flexible network technology that lends itself as a cost-effective solution for connecting instruments, cameras, and computers in challenging facility environments. Network nodes currently used in this type of application provide channel authentication, the hardness of which will be increased to 128-bit strength in the very near future. Although not a one-size-fits-all solution, free topology provides for the flexible implementation of safeguards equipment in a variety of facilities.

References

[1] Robert F. Parker, et al.: Integrated Monitoring Hardware Developments at Los Alamos, Los Alamos National Laboratory Document, LA-UR-99-2053 (1999)

[2] James K. Halbig, et al.: Integrated Monitoring System—An Overview, Los Alamos National Laboratory Document, LA-UR-99-2109 (1999)

---

[1] *Securely*, in this case, refers to data which have been authenticated and/or encrypted.

[2] LON (Local Operating Node – trademark of Echelon Corporation)

[3] A technique to reduce memory usage by condensing statistically indistinguishable data points to a single point

[4] Authentication refers to a means of digitally certifying the sender of a block of data, such as a digital signature.

[5] Link refers to an uninterrupted (no repeater) connection between two nodes in a network.

[6] RAID (Redundant Array of Independent Disks) is a commonly used reliable mass storage technology.