Remote Monitoring in Safeguards: Security of Information and Enhanced Cooperation

Galdoz, E.; Calzetta, O.; Fernández Moreno, S.; Llacer, C.;
Díaz, G.D.; Vigile, S. and Brunhuber, C.

Presentado en: INMM 52nd Annual Meeting.
Palm Desert, EE. UU., 17 al 21 de julio de 2011

REMOTE MONITORING IN SAFEGUARDS: SECURITY OF INFORMATION AND ENHANCED COOPERATION

Erwin Galdoz[1], Osvaldo Calzetta[1], Sonia Fernández Moreno[2], Carlos Llacer[2], Gustavo Díaz[2], Sebastián Vigile[2], Christoph Brunhuber[3]

[1]ABACC - Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials, Rio de Janeiro, Brazil

[2]Argentine Nuclear Regulatory Authority, Buenos Aires, Argentina

[3]IAEA – International Atomic Energy Agency, Vienna, Austria

ABSTRACT

Unattended systems with remote transmission capabilities (RM) have the potential to improve safeguards efficiency. Moreover, the evolution of technology and the steady growing of nuclear materials subject to control, lead modern safeguards increasingly utilizing unattended equipment with the capability to store relevant data for long periods of time coupled with the option of being remotely accessed and checked. Remote inspection is still a concept under development, but it may end to be a powerful more efficient verification modality in medium term future. An important part of drawing meaningful safeguards conclusions rests on authenticity and reliability of the information on nuclear material and facilities acquired through the various verification activities and measures applied by IAEA and regional safeguards organizations, like ABACC.

The increasing utilization of such technology to further optimize safeguards responds to a multifaceted environment where security of information for all relevant parties is of utmost importance. From the point of view of the IAEA and ABACC, the use of any technology for safeguards application, and specially the use of RM, requires to ensure the security of data collected to guarantee the validity and veracity of such information throughout the whole process (e.g., from collecting to reviewing). This is also valid to the SSAC involved in the process. Information security is also relevant for States and Operators. Assurance should be given that the information could not be withdrawn by non-authorized entities and that facility data is also fully secured. Another important aspect related to RM that may also fall in the security aspect of safeguards relevant information that merits further consideration, is the sharing of information between organizations like ABACC and the IAEA as well as the possibility to make this data available for States authorities purposes.

This paper discusses three main themes related to RM: (i) the extent to which security is key for RM application acceptance and use for the IAEA, ABACC, States and Operators, ii) the sharing of relevant safeguards data for all the parties concerned, iii) a scheme agreed between ABACC and ARN to trial a RM transmission and a possible approach for international safeguards application.

REMOTE MONITORING APPROACH

Safeguards implementation is essentially a technically driven process, in which large amounts of data, sometimes of radically different nature, must be collected (i.e. nuclear or non-nuclear measurements, surveillance images, conventional or electronic support documents), verified for safeguards purposes (using specific authentication techniques), stored (in different storage media like magnetic tapes, memory cards, removable hard drives, optical disks), secured (using encryption and/or authentication techniques), transported (carried by the inspector, or transmitted over public communication lines) and finally analyzed (by data comparison, measurements evaluation, images review, etc.) using different techniques and grades of precision, depending on the specific facility

approach. All of these, for a large and increasing number of facilities around the globe. This brief summary seems to show heterogeneous, complex and cumbersome data management scenarios. And so it is.

Increasing efforts are continuously made to introduce new technology in order to reduce or minimize the complexity and costs involved in this process, thus increasing the efficiency without compromising the effectiveness, precision and completeness of the verifications performed.

One of the important efforts consists of the transmission of the information collected by communication capable devices running at the monitored facilities to servers located at the monitoring agencies headquarters, where inspectors can analyze the data in detail using software tools aiding the job, and gather conclusions in a more efficient and less intrusive way. This is the basic idea of Remote Monitoring Systems, in which unattended monitoring equipment, such as optical surveillance systems, are connected to a central storage system using any available communications link, to transmit the collected information. The information must be properly conditioned prior to be transmitted over publicly accessible lines, by encrypting and digitally signing the data packets, as described later.

SECURE TRANSMISSION: DIFFERENT PERSPECTIVES AND REQUIREMENTS

Several security requirements must be met when any piece of information is to be transmitted over a publicly accessible line, to ensure the data shall reach its intended destination unaltered, the originator identity can be authenticated, and no access to the information by unauthorized third parties is possible while transmitted through public lines.

In the general case of Remote Monitoring Systems for safeguards application, the data is originated in equipment under control of an organization intended to receive and process it in a different place, that is, the monitoring agency. Authentication techniques should be applied immediately after the data is produced to reduce the risk of data tampering. When two organizations or more share the equipment and its data under certain agreed procedures for joint use, they have also to agree on how to apply and fulfill the above-mentioned requirements.

To securely transmit the information to the final destination, two different approaches can be considered. The first is based on the use of a private communication line. This approach is nowadays still expensive and difficult to implement. The second approach uses normal communication lines like telephone lines or internet links, as a physical layer. The information must be encapsulated using strong encryption and authentication techniques, widely available in reliable and inexpensive VPN (Virtual Private Network) implementations. Using this approach, even network infrastructure owned by the Facility Operator (FO) or the National Authority (NA) can be employed, not compromising the system trust.

Not only should the perspective of the monitoring agency be taken into consideration, but normally the FO and/or the NA have also conditions that must be met in order to accept the RM approach. The NA is required to protect the information taken from nuclear installations for security, industrial and technological aspects, among other reasons. In this regard, the NA should be able to ensure and demonstrate that the information transmitted is that agreed upon, and also that the equipment cannot be remotely accessed in order to modify parameters without prior agreement. Therefore, to implement a RM application it is also important to satisfy the State/Operator security requirements.

SHARING OF DATA: ANOTHER IMPORTANT CONSIDERATION

Successful safeguards implementation depends on the cooperation of all parties concerned. In the case of a RM application, that implies the IAEA and ABACC, the NA and the FO.

The existence of a robust and effective SSAC empowered with the necessary legal authority, which is independent from operators, and has adequate resources and technical capabilities to administer the requirements of safeguards agreements to properly verify nuclear material accountancy and control systems at nuclear facilities and LOFs is of utmost importance.

All involved Agencies (i.e. IAEA, ABACC, and the NA) should discuss and agree procedures to allow the sharing of data to the fullest extent possible. This criterion should not compromise a relevant diversion scenario.

Simultaneous full sharing of the information transmitted with the NA may be considered as difficult to accept for the Agencies. However, there is the possibility of sharing data in a way that would not compromise the safeguards approach. For example, let us consider the situation when the amount of data and due time are such that a surveillance malfunction or potential flaw, relevant for the approach, can be disclosed without negative impact on the evaluation. This is a scheme that would allow all parties to obtain the fullest possible benefits of RM applications.

JOINT REMOTE MONITORING BETWEEN IAEA AND ABACC

A more technically complex situation involves multiple agencies jointly monitoring several facilities, and that is the case of ABACC-IAEA joint safeguards. As noted above, in this case both agencies share the information collected by unattended surveillance equipment, owned by one of the agencies, but provisions must be ensured so both agencies can obtain independent conclusions.

Once the information is acquired and conditioned, it is simultaneously transmitted to the agencies´ headquarters for further storage, analysis and review. Parallel VPN channels should be used for secure transmission.

Another feature to be considered is that corrective or preventive maintenance tasks must be done when some malfunction is detected. In some occasions this can be done remotely. In this situation there are requirements from both the NA and the agency which does not own the equipment that need to be adequately addressed. One condition to be met is that even when the owner agency is responsible for accessing the system for maintenance purposes, the other parties involved must be aware of the access, and able to audit the access to avoid undesired or not agreed changes that could affect the system operation and/or performance.

A VARIATION: STATE OF HEALTH REMOTE MONITORING

Depending on the nature of the facility under monitoring, the State can require safeguarding industrial, commercial or national security related aspects to the extent that the information gathered by the surveillance systems is not to be retrieved outside the facility. All review activities must be performed during the inspection time, inside the facility boundaries, and the conclusion must be obtained prior to leave the installation.

Even if that is the case, remote transmission of relevant information indicating the State of Health (SoH) of the equipment and components, excluding any sensitive information, can significantly improve the overall system performance and efficiency, by allowing prompt alerts when

malfunctions occur, or symptoms announcing such malfunctions are detected. As a result, safeguards intrusion and inspection effort can be reduced.

The security considerations are essentially the same as in the full Remote Monitoring implementation, but the State normally may require extra auditing capability over the transmitted information.

SoH DEMONSTRATION TEST BETWEEN ABACC AND IAEA

A demonstration experimental set-up is being tested between the ABACC and the IAEA, where the SoH information gathered from an SDIS surveillance system (owned by and located in ABACC HQ) and two NGSS cameras (owned by IAEA, also located in ABACC HQ) is simultaneously transmitted to both agencies storage sites for further analysis. Symmetrical remote access to the monitored surveillance system for maintenance purposes is also granted. By symmetrical access must be understood that no agency can remotely access the system without effective acknowledge of the other, and all activities can be monitored in real time, as explained later. All communications that use public Internet services are encapsulated inside VPN tunnels.

The traffic is managed by the firewall rules set-up in the VPN devices participating in this multi-tier communication scheme. The VPN devices selected for this project are all qualified by the IAEA for remote transmission of safeguards data. The applied VPN rules define which data paths are permitted, in which direction, and what services (i.e Transmission Control and Internet Protocols, TCP/IP services) are expected to be used. All other traffic is denied by default. In this way, it is assured that all data are sent to the intended destination servers only, and only the authorized computer, with the proper temporary permits granted, can access the surveillance system. Access to the VPN devices configuration is controlled by passwords shared by both agencies, ensuring that changes can only be done jointly.

Figure 1 shows a scheme of the network configuration between the simulated facility and both agencies sites. The surveillance system (A) is connected to Internet by using a dedicated ADSL link, simulating the connection type normally available at facilities. The Joint RM Server (B) is connected to the Internet using ABACC regular Internet provider, and identified by a public IP address. The ABACC RM server and Joint RM Workstation (C) are also connected through the same provider and using a different public IP address; and finally, the IAEA RM server (D) is also connected to Internet using regular Internet resources at IAEA HQ. In this way, a realistic communications scenario is fully simulated. This Joint Use Server approach has been successfully in use for more than three years between IAEA and EURATOM.

Only the computer labeled as Joint RMS Workstation is allowed to initiate a Remote Desktop session at the monitored SDIS server and that access is controlled by the IP Tracking VPN device (See details in Annex 1). In that way, a session can be initiated only if the access is remotely granted from within IAEA HQ. In the same way, IAEA can only start a session from within that workstation, and the access is granted by ABACC simply by turning the Workstation on. This scheme allows a completely symmetric access right, and all maintenance activities must be carried out jointly, as requested by design.

The surveillance system (A) also includes an extra computer identified as Traffic Recording Device, which works as a proxy between the monitored systems and the rest of the network. This proxy computer runs ad-hoc software developed by IAEA, which intercepts all traffic coming from and

going to the monitored system, and all that traffic is recorded for auditing purposes prior to be dispatched to the intended destination. These auditing records are stored on the recorder hard drive, and can be requested by the FO and/or the NA at inspection time to verify that only the agreed information was transmitted during a previous period under review.

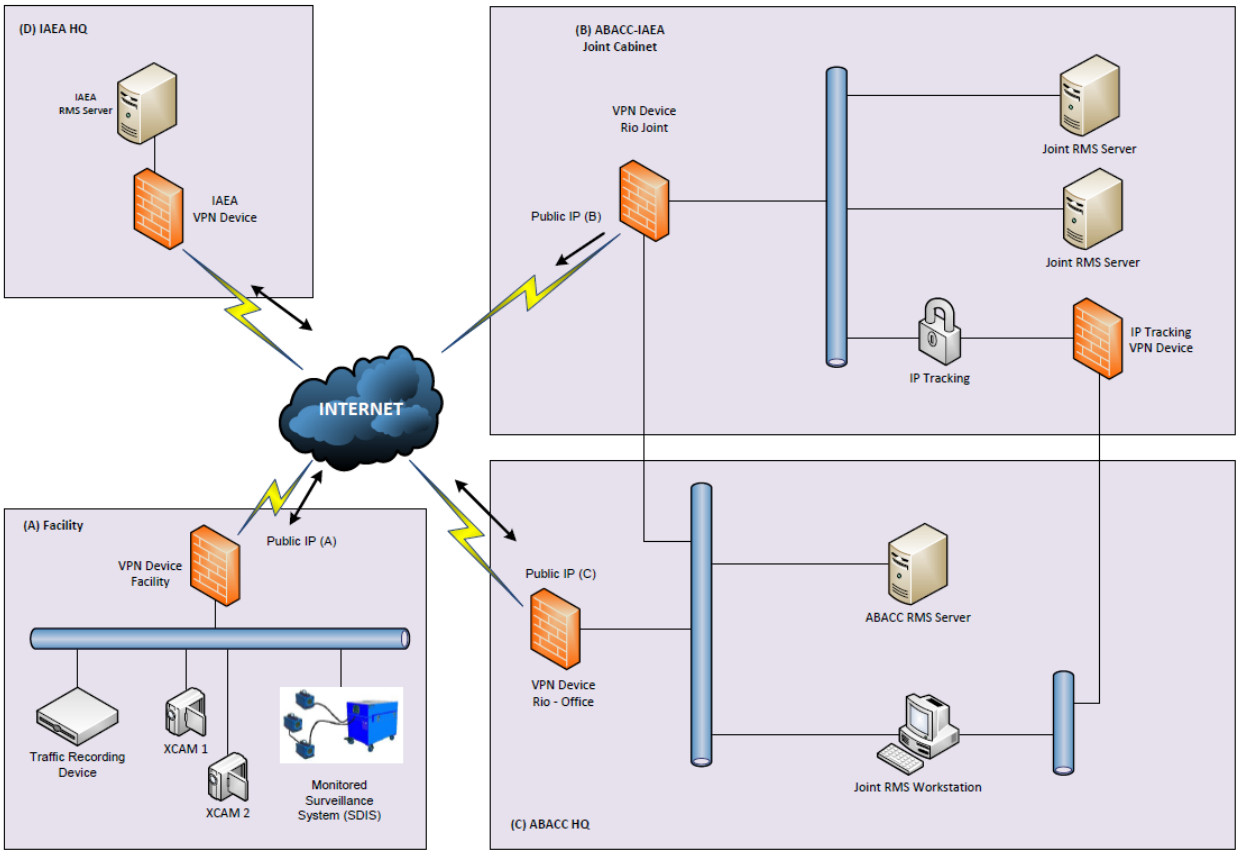

Figure 1: Network diagram of the Joint SoH demonstration pilot.

SoH TRANSMISSION FROM THE PERSPECTIVE OF THE NA

The VPN approach proposed in this paper makes the use of network infrastructure provided by the National Authority (NA) possible. Therefore it is a preferable option as the NA is responsible for the access to the facility since the use of the FO/NA network does not compromise the reliability of the system and fulfills the other Monitoring Agencies requirements. This would also allow the NA to keep a log of transactions time, direction and amount, which would be used to verify at accorded time that the agreed data was effectively transmitted and that all data flowed outward and not inward.

It is necessary to keep in mind that due to security concerns, encrypted data is usually not allowed to flow through the FO/NA network. In order to route this encrypted data some rules should be enforced on the equipment. To achieve these data paths, TCP/IP services and the data flow intended direction should be agreed with the NA.

To complement this, as in the ABACC-IAEA test previously mentioned the surveillance system (A) also includes an extra computer identified as Traffic Recording Device, as explained above.

OTHER VARIATION: FUTURE IMPLEMENTATION AND UPGRADE

In the future, the development of a RM scheme capable of corrective or preventive maintenance tasks could be forethought. In some occasions these corrective or preventive maintenance tasks could be done remotely. In these cases, there are requirements from both the NA and the agency that does not own the equipment that need to be adequately addressed. One condition to be met is that even when the owner agency is responsible for accessing the system for maintenance purposes, the other parties involved must be aware of the access, and able to audit the access to avoid undesired or not agreed changes that could affect the system operation and performance. Also, as each and anyone of these accesses may affect the RM system performance and/or the collected data integrity, they should be previously agreed with the NA. For the same reason, all incoming data flow should be logged for eventual review.

In the Figure 1, with public IP (A) provided by the NA, only the computer labeled as Joint RMS Workstation is allowed to initiate a Remote Desktop session at the monitored SDIS server and that access is controlled by the IP Tracking VPN device. In that way, a session can be initiated only if the access is remotely granted from within IAEA HQ. In the same way, IAEA can only start a session from within that workstation, and the access is granted by ABACC simply by turning the Workstation on. According to the scheme proposed, and as the NA supervises the connection to the facility, a completely symmetric access is granted, and all maintenance activities must be carried out jointly, as requested by design.

Some tools to store and replay the Remote Desktop sessions performed by the agencies with maintenance purposes have also been successfully tested. Such tools allow the auditing authority to easily verify the tasks carried out on the surveillance server should such sessions have occurred during the surveillance period under review.

CONCLUSIONS

The preliminary results of this demonstration test involving a multi-agencies remote monitoring system with delayed auditing capability show that the system as depicted is reliable, and all design requirements of security and access permits granting are fulfilled, assuring that all parties can verify the proper use of the system, without compromising the reliability and data confidentiality. The ad-hoc proxy software involved is simple enough, and the security and recording phases are implemented using commercial off the shelf software that can be independently assessed by any of the parties involved in the project.

ANNEX 1: WHAT IS “IP TRACKING”?

The Juniper VPN device has a special feature called “Interface Failover with IP Tracking”. The manual tells us: “You can specify that when certain IP addresses become unreachable through the primary Untrust zone interface, the security device fails over to the backup Untrust zone interface even if the physical link is still active. ScreenOS uses Layer 3 path monitoring, or IP tracking to monitor IP addresses through the primary interface. If the IP addresses become unreachable through the primary Untrust zone interface, the security device considers the interface to be down, and all routes associated with that interface are deactivated. When the primary Untrust zone interface changes to the down state, failover to the backup Untrust zone interface occurs.”

We use this feature for the following approach: The IP Tracking device (access device) located in the sealed cabinet is the only network path into the sealed cabinet. The device has two Untrust

interfaces. The second one is not connected. The primary interface is connected to the main VPN device in the cabinet which maintains tunnels to the facilities and to IAEA and ABACC. The access device tracks the IP address at the remote endpoint in IAEA HQ. The IP packets are traveling from the access device via the main VPN device through the tunnel to Vienna. By not responding to the ping, the access into the cabinet can be cut from Vienna.

ABACC has direct access to the access device, so ABACC must not have the ability to change the access device configuration. In other words ABACC must not have the ability to switch off IP Tracking.