Secure Video Surveillance System (SVSS) for Unannounced Safeguards Inspections

Richard L. Lucero, Jack C. Bartberger, Diana Eichert[1], Mark Pinkalla, George Baldwin
Sandia National Laboratories[2]
PO Box 5800
Albuquerque, NM 87185-1377
e-mail: rllucer@sandia.gov, jcbartb@sandia.gov, deicher@sandia.gov, mnpinka@sandia.gov, gtbaldw@sandia.gov

Erwin Galdoz, Geraldo Renha, Max Facchinetti
Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials (ABACC)
Av. Rio Branco 123, 5to Andar
CEP 20040-005 - Rio de Janeiro, RJ, Brazil
galdoz@abacc.org.br, grenha@abacc.org.br, facchine@abacc.org.br

Abstract

The Secure Video Surveillance System (SVSS) is the product of collaboration between the U.S. Department of Energy (DOE), Sandia National Laboratories (SNL), and the Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials (ABACC). The joint project addresses specific requirements of redundant surveillance systems installed in two South American nuclear facilities as a tool to support unannounced inspections conducted by ABACC and the International Atomic Energy Agency (IAEA). The surveillance covers the critical time (as much as a few hours) between the notification of an inspection and the access of inspectors to the location in facility where surveillance equipment is installed. ABACC and the IAEA currently use the EURATOM Multiple Optical Surveillance System (EMOSS) which is now out of line and no longer supported by the manufacturer. In addition, spare parts are no longer available. The redundant systems currently used so far have properly attended the expected objective, but ABACC and the IAEA are concerned that the risk of complete failure is unacceptably high. A maintainable, current-technology solution is needed urgently. As a field test, ABACC intends to replace one of the existing ABACC EMOSS systems by the Secure Video Surveillance System (SVSS). SVSS utilizes commercial off-the shelf (COTS) technologies for all individual components. Sandia National Laboratories (SNL) supported the system design for SVSS to meet Safeguards requirements, i.e. tamper indication, data authentication, etc. The SVSS consists of two video surveillance cameras linked securely to a data collection unit. The collection unit is capable of retain historical surveillance data for at least three hours, with picture intervals as short as 1sec. Images in .jpg format are available to inspectors using various software review tools.

[1] Global Analytic IT Services

[2] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Motivation for a New Surveillance System

The ABACC, jointly with the IAEA, routinely performs safeguards activities at nuclear installations in Brazil and Argentina. In some of these facilities, the ABACC and IAEA utilize a special type of surveillance measure during unannounced inspections. Currently, the EMOSS (EURATOM Multi Optical Surveillance System), developed by EURATOM for the IAEA, is the surveillance technology employed. The EMOSS is out-of-date and no longer manufactured, which has presented difficulties in purchasing spare parts and performing system maintenance. It is increasingly prone to failure. The ABACC therefore desires a replacement system, specifically designed to fulfill unannounced inspections requirements.

The IAEA has been developing the Next Generation Surveillance System (NGSS), which eventually will replace existing safeguards surveillance systems. However, the NGSS is not yet in production, and it is not known when NGSS units would replace the EMOSS.

The ABACC and the U.S. Department of Energy (DOE) therefore agreed to develop a surveillance system using current commercial off-the-shelf (COTS) technology, customized to comply with the specific requirements for the unannounced inspection application. The solution would ensure data redundancy, confidence, and system reliability, with a relatively low cost for development, construction, operation, and maintenance.

Application Requirements

The safeguards approach for unannounced inspections requires that a well defined perimeter entrance is kept under surveillance between the time inspectors request access and the time they finally arrive at that entrance. The time interval is currently agreed to allow the operator to protect what he considers as sensitive information. Therefore, the surveillance system may only retain images acquired during the previous few hours. Furthermore, in the case where inspectors gain access in less than the agreed time, all images acquired prior to the inspection request must not be visible to the inspector.

The goal of the surveillance is to detect small quantities of nuclear material exiting the perimeter, which could happen quickly, due to the reduced space available to establish the surveillance field of view. The requirement is therefore a Picture Taking Interval (PTI) (between successive surveillance frames) of one second.

ABACC and IAEA inspectors may review the surveillance record either jointly or independently during unannounced inspections. All review activities must take place on site; no images may be removed from the facility. The surveillance system must therefore provide the inspector with all software tools necessary to obtain a safeguards conclusion prior to leaving the facility. In case of inconclusiveness or doubt, it must be possible to store the images on external media, kept under both ABACC and IAEA seals, under the operator control, for further discussion.

Images are acquired by two independently-positioned cameras and are transmitted over a wire link to a collection unit for storage and review. The link must be protected using strong authentication

measures to ensure that legitimate images are reviewed during inspections. The camera housings and collection unit must include tamper indication to detect any illicit activities.

To increase system reliability, images must be retained also within the camera housing for backup purposes. These backup images would only be needed as a last resort to recover surveillance in the event of collection unit or transmission failure. Emergency procedures must be defined to allow the inspector to obtain safeguards conclusions without violating the confidentiality required by the operator.

The system will operate on facility main power coming from a secured facility line. However, an uninterruptable power supply (UPS) within the tamper-indicating enclosure is required to protect against short-term loss of power. The UPS will further ensure that the cameras have priority to operate autonomously.

SVSS: Design Approach

The design relies on the use of commercial, off-the-shelf (COTS) components to build the system that complies with the stated requirements.

There are a number of cameras with different features that can be used for the intended purpose. A network camera designed for surveillance was selected for the SVSS system. This camera is capable of acquiring and collecting images via Ethernet at a one second or greater PTI. It is also capable of storing images locally on removable flash memory.

The images acquired by the camera modules are transmitted (pushed) to a collection computer, or server. The data transmission is handled by an Ethernet connection between each camera and the server. To ensure that the images stored in the server for review are authentic and were generated by the correct cameras, the transmission is encapsulated inside a VPN (Virtual Private Network) tunnel, implemented with VPN hardware devices already approved for safeguards purposes.

To confirm that no tampering has occurred in the system, the camera enclosures and server cabinet are sealed, using appropriate seals to permit independent access of only one agency (IAEA or ABACC) during inspections. The cabinet selected to enclose the server computer is a two compartment Hoffman enclosure, accessed by independent doors. The bottom door is sealed with a passive metallic seal and is intended to access the main system components for maintenance purposes only. The other door (top), is sealed with an electronic seal (VACOSS or EOSS), which allows the inspector to access the server computer during a surveillance review by using the keyboard and monitor.

The collection computer is an industrial PC running standard software for storage and review of the images, according to the requirements. Specific software operates on the server to maintain at least a few hours of data available for the inspector to review, two hours for instance. The software also downloads the jpeg-format images from the camera(s) and converts the images into an .avi file for playback review during the inspection activities.

In case of a communication failure, a procedure runs automatically to retrieve the images after the system recovers, ensuring the information is available when the inspector arrives at the system. In case of a system failure, it is possible for an inspector to retrieve the images directly from the local removable flash memory, for conditioning and safeguards review.

Safeguards technical data are also recorded on the system. A file is produced and continuously updated, containing abnormal events that may have occurred during the period between two consecutive inspections, such as power outage events, cameras or server housings opening events, high temperature alerts, etc. These events are shown to the inspector for feedback on reliability and performance of the system.

A UPS provides uninterruptable power to the system, to ensure that a power outage does not cause an interruption of the surveillance process. The UPS is designed to provide power to the system continuously. If the power outage persists, the UPS will begin shutting down all hardware components except for the cameras, which will use the remaining battery power for image collection.

The diagrams in figures 1 and 2 show the main components of the system and their interconnection. The photographs in figure 3 show the prototype cabinet with the inspector door opened (at left) and closed (at right), and the closed cameras housings on top.

Software Architecture

The system is designed using a client server model, where the cameras act as clients producing images and the server receives and stores the images pushed periodically by the client's cameras.

A two layer software platform operates in the server computer:

- A Linux based layer that receives and stores the images in the server hard disk. Also the images older than the time-limit are removed at this level. Technical events are also processed and recorded in this layer.
- A Windows based layer, which operates as an interface to the inspector, and allows the images review.

Both operating systems run on the same computer, by using VMWare to share resources.

The inspector layer is used by the inspector to run review software. In a first stage, a standard utility will be used to play AVI files. The AVI files will be generated by taking the images stored, covering the period under surveillance only.

In the production system it is foreseen to use software specifically designed for safeguards review of surveillance, such as GARS, which can be configured to handle the images generated by SVSS cameras.

Prototype Tests

A first prototype was built at SNL following the requirements specified above. ABACC and SNL defined a suite of acceptance tests to be performed prior to installing the system for a field trial.

The tests were defined to verify system behavior, according to the following criteria and parameters to be observed:

- Design Requirements Compliance:
  - Safeguards: PTI, storage time restriction, network security and data authentication, safeguards images review procedures, crash recovery, tampering indication, etc.;
  - Electromechanical issues: Power supply, enclosures, seals, etc.
- Performance:
  - Images quality;
  - Disk usage and performance;
  - Images transfer time.
- Reliability:
  - Mechanical and electrical robustness;
  - Thermal limits;
  - Network reliability;
  - Hard drive reliability;
  - Flash memory reliability;
  - UPS reliability and capacity.

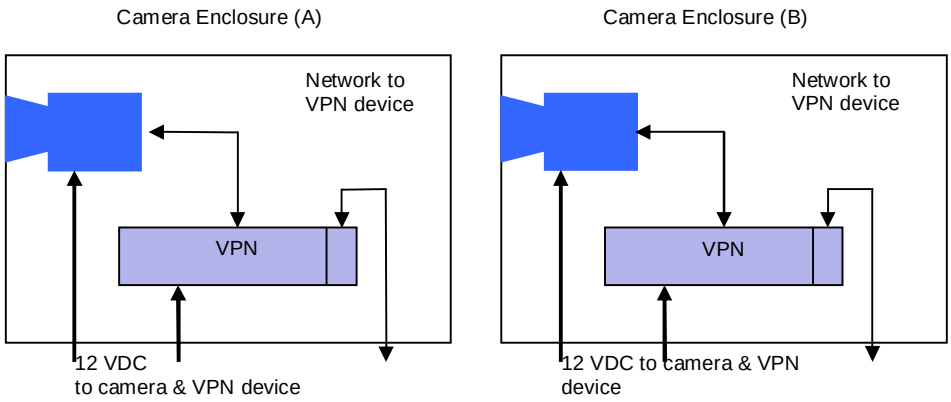

Figure 1: Functional diagram of the camera modules.

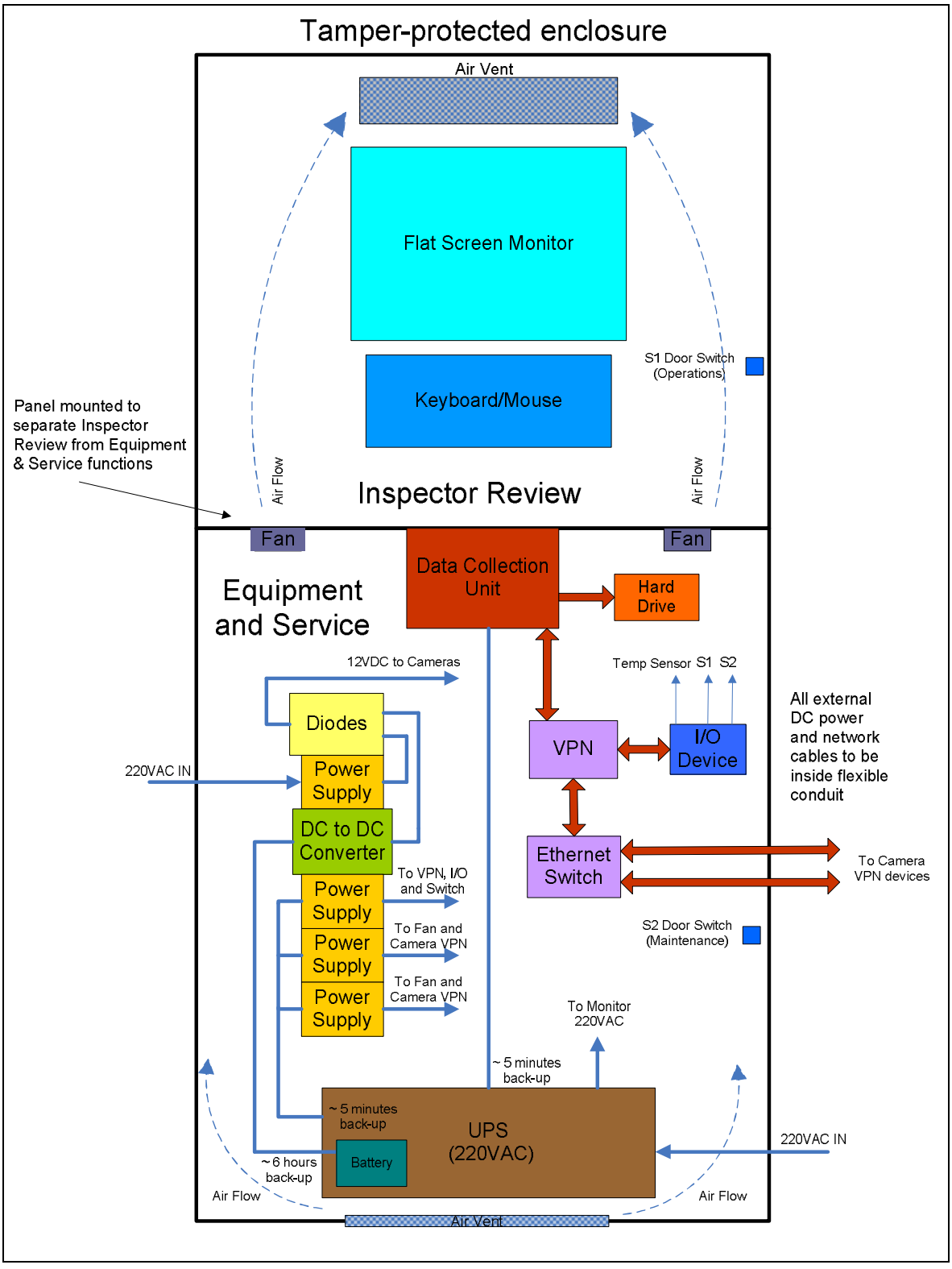

Figure 2: Functional diagram of the SVSS server.

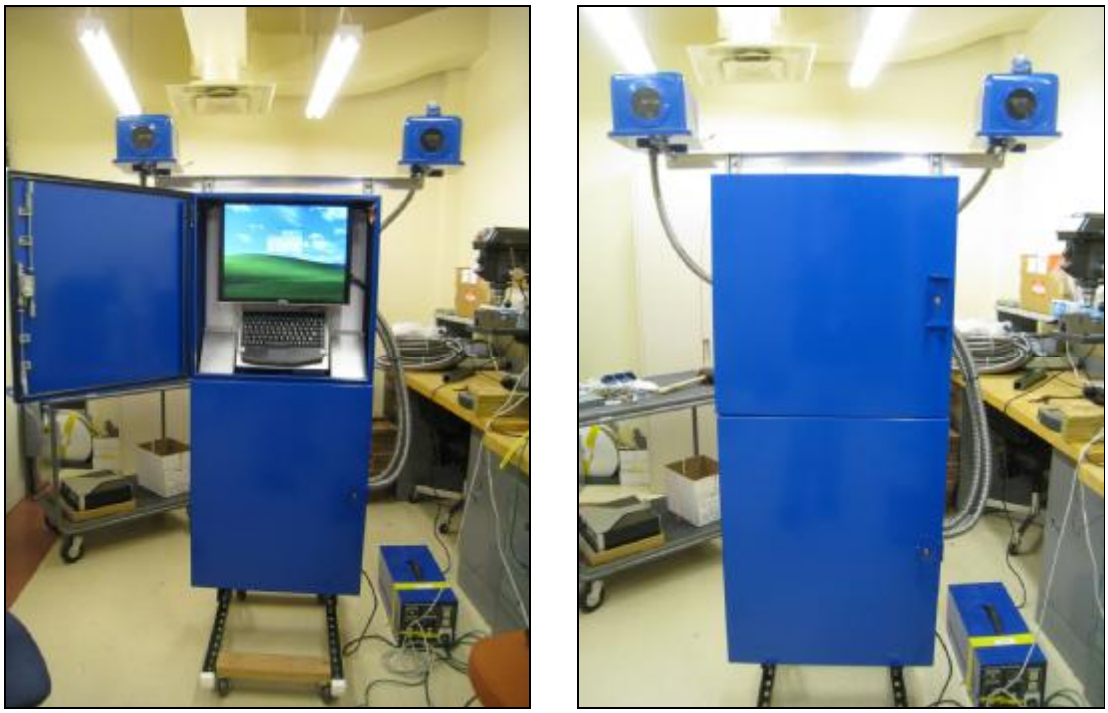

Figure 3: Pictures of the SVSS prototype.

Conclusions

Some adjustments in the design were suggested as a result of the tests already performed. Further tests are still pending. The preliminary results are highly satisfactory, and the proposed design proved to be acceptable for the intended purpose.

The next steps include the final stages in the assembly of three units. The original development prototype will remain at Sandia National Laboratories. A second unit will be installed and operated at the ABACC Safeguards Laboratory and the third one will be installed by ABACC at a facility for a field trial. The SVSS system at the ABACC lab will be used for performing additional testing, training of new technical and inspector staff, maintenance, and continued safeguards operation. It is foreseen to perform tests jointly with the IAEA which may eventually desire joint use for the intended safeguards application.

Also, it will be requested to the manufacturer of GARS review software to adapt a version capable to handle SVSS images, in order to provide the inspector a well known tool for surveillance review.

Acknowledgment

The authors greatly appreciate both the programmatic and financial sponsorship for this work that was provided by ABACC and the U.S. Department of Energy, National Nuclear Security Administration's International Nuclear Safeguards Engagement Program (INSEP). We especially thank John McClelland-Kerr and Alex Sunshine for their support.