Development of Next Generation Advanced Remote Monitoring System

Rustem Samigulin, Sergey Blagin, Vladimir Angilopov, Alexey Veselov, A. Kokoulin
All-Russian Scientific Research Institute of Experimental Physics (VNIIEF), Sarov, Russia

Dennis Nelson
Sandia National Laboratories, Albuquerque, New Mexico, USA

Abstract

The paper describes the latest upgrades for the Advanced Remote Monitoring System (ARMS) designed for monitoring access to a fissile material storage facility, as well as providing a remote, highly reliable intrusion warning system.

ARMS is a self-contained monitoring system. The single enclosure contains motion detectors, stationary video cameras, a web server, uninterruptible power supply, radio frequency (RF) communication capability, and Controller Area Network (CAN) and Ethernet interfaces. In the free-standing mode, the box is mounted on the vault ceiling to monitor access to protected areas. Event detection data is stored on the server, assigned a digital signature, and then transmitted via the Internet to remote user terminals. An International Atomic Energy Agency (IAEA)-approved algorithm is used for authentication of transmitted information.

The ARMS can incorporate the RF tag system as remote sensors. It can also receive signals from additional external sensors via a CAN bus and incorporate real-time video surveillance using the Internet.

Introduction

As part of the Warhead Safety and Security Exchange (WSSX) Agreement Program, the All-Russian Research Institute of Experimental Physics (VNIIEF), in cooperation with Sandia National Laboratories (SNL), has developed the following various technologies for nuclear material storage applications:

- Facility-to-Facility (F2F)
- RF Tag Authentication, Encryption, and Motion Detection System
- Ethernet controller
- Pedestrian portal radiation monitor
- Web-camera and barcode reader

The new ARMS design integrates all previously developed and enhanced technologies into a system that improves performance and user-related characteristics of non-radiation monitoring techniques. ARMS can operate either in a stand-alone mode, or as part of the F2F system. It acquires and stores data from RF tags, mobile barcode readers, pedestrian portal radiation monitors, Ethernet controllers, and external sensors connected through a CAN dual-wire bus.

Sandia National Laboratories 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-AC04-94AL8500.

Distinguishing features of the advanced remote monitoring system include the following:

- validated access registration
- video surveillance cameras
- built-in Ethernet controller
- nonvolatile memory
- CAN bus operation support
- built-in RF capability
- data storage server and Web server
- highly reliable authenticated data transmission channel
- protection of information from deliberate distortion during transmission
- uninterrupted operation in case of external power failure
- small enclosure dimensions

Background

One of the IAEA requirements for remote monitoring systems deployed in nuclear material storage facilities is data authentication capability. Data authentication prevents data tampering and permits distant users to utilize remote monitoring methodology. However, a large number of different types of sensors introduces a new data acquisition and storage problem. In addition, for authentication and interfacing with data storage server purposes, a microcontroller has to be added to each sensor. To address this problem, we developed a technology that integrates key sensors into a single platform. This is a stand-alone unit that includes an optimized set of sensors and a data storage system, and provides authentication of information transmitted to the user. The platform design, by replacing individually installed sensors, reduces equipment and installation costs. During the first phase of the project, we developed a remote monitoring system that included several different sensors contained in a single housing, and a separate data collection server installed on a personal computer (PC). The system was successfully tested in the F2F Russian Demonstration Facility, which enabled us to proceed to the next phase: development of an advanced remote monitoring system that includes a data storage server.

ARMS Description

The ARMS is a device that performs surveillance of a vault using motion sensors and video cameras. The ARMS is installed on the ceiling, and it controls the lower 2π sphere of the 10x10 meter square area with a 3-meter high ceiling.

The ARMS design is shown in Figure 1.

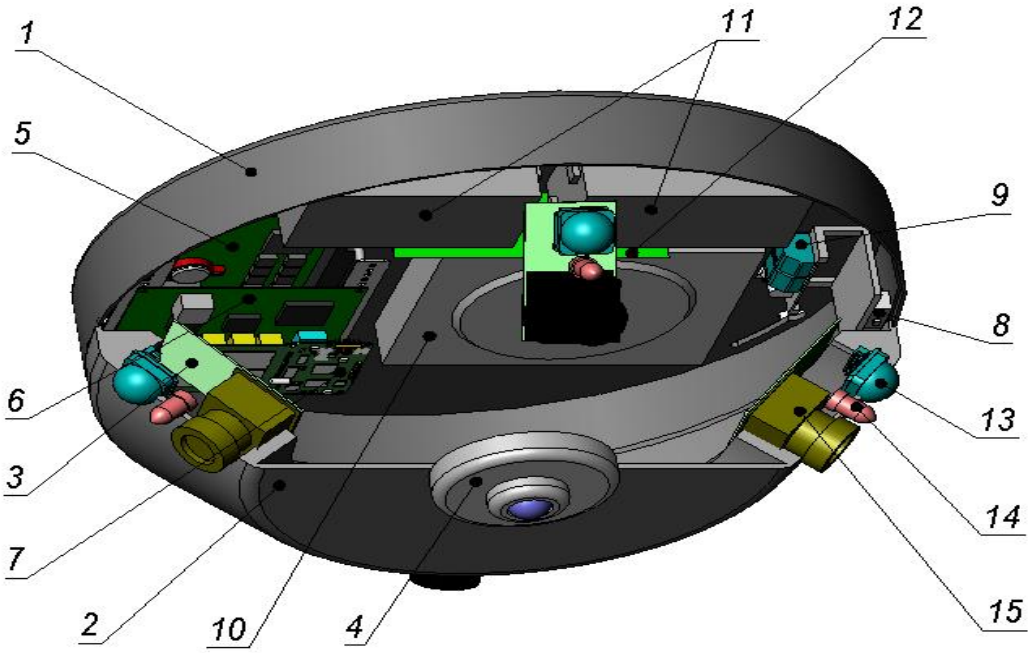

Figure 1: ARMS Design

The ARMS includes:

1. A housing base support made of D16-T alloy
2. A housing cover made of RF-transparent polymer material
3. Four sensor modules located along the housing perimeter
4. An infrared (IR) sensor Octopus EP with 360° coverage angle
5. A master controller WAFER-LX-800
6. A video controller Aviosys IP Video Server 9100A
7. An RF module 916MHz
8. A tamper indicating device that also serves as a dismantlement sensor
9. Power connectors 12-24V, Ethernet, CAN
10. A hard disc CF-1GB
11. Two backup batteries 7A/hr
12. A power source with battery charger HESC-104+

The sensor modules (#3) include:

13. An IR sensor CON-PIR-STD with 120° coverage angle
14. Lighting
15. A video camera VIEWSE VC-807L + lens with 120° field of vision

Monitoring the room requires two types of detection technology: IR motion detectors and a video surveillance system. This approach makes the system more robust and resistant to attempts to conceal tampering. Four IR detectors are located along the sphere's perimeter to provide 360° monitoring. To supplement and support the veracity of recorded events, an additional IR detector with 360° field of vision is installed in the center. Its function is to provide redundant indicators and emergency monitoring in the event that the four other IR detectors fail. Four video cameras hooked up to the video controller provide continuous video monitoring of the room and record any movement within their field of vision. The video controller converts the analog signal from the video camera into the .jpg format. The video controller compares frames, identifies movement in the video frame, and records access.

The ARMS housing is designed to prevent access to internal components without physically destroying the housing or triggering the dismantlement sensor. The dismantlement sensor records unauthorized access to the ARMS internal space to prevent falsification of IR sensor and video camera data.

The RF module collects data from RF devices included in the system for storage facility applications (RF Tag Authentication, bar code reader). The ARMS can support an additional set of external sensors connected by the CAN serial bus. This two-wire bus provides power supply to external sensors and supports data exchange at the same time. CAN supports concurrent connection of several dozen sensors to one pair of cables, which significantly simplifies the process of installing additional sensors. ARMS includes backup batteries that are capable of supplying required power for two hours in case of power failure. Data from IR detectors, the video controller, external sensors, and the dismantlement sensor are sent to the master controller. The ARMS block diagram is presented in Figure 2.

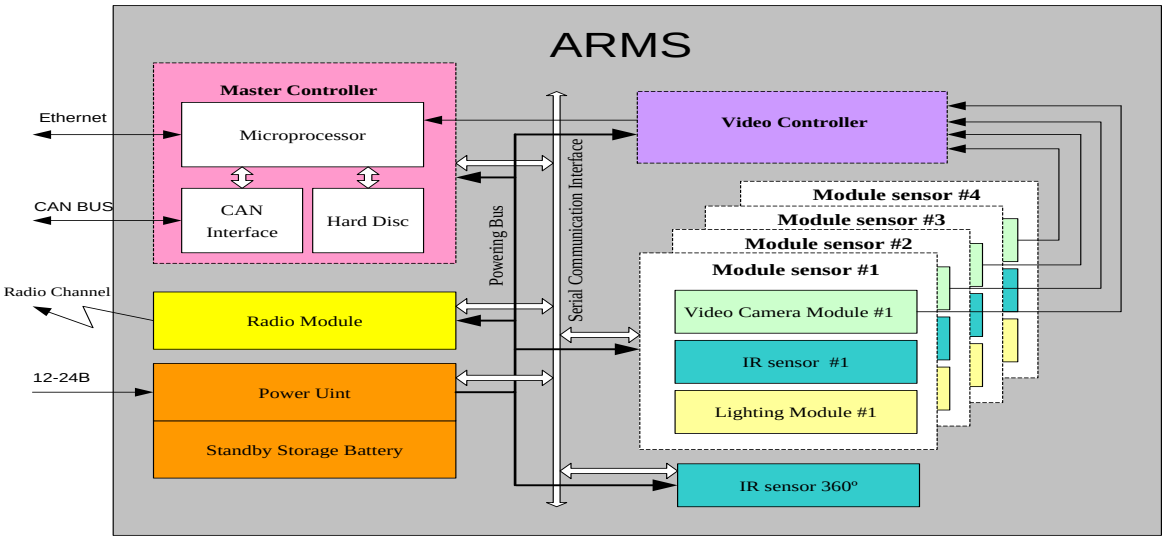

Figure 2: ARMS block diagram

The master controller analyzes sensor data, identifies the type of the event, and records the event in the database.

The data stored in the database can be accessed by remote users via the Internet network. A remote user can view data in the database at any time, and can retrieve information about any events that may have occurred in the storage facility.

The data validity is ensured with authentication. The data is authenticated using the hash function calculation algorithm Secure Hash Algorithm (SHA-1) applied in the Digital Signature Algorithm (DSA). The principle of authenticating data transmitted from the ARMS is presented in Figure 3.

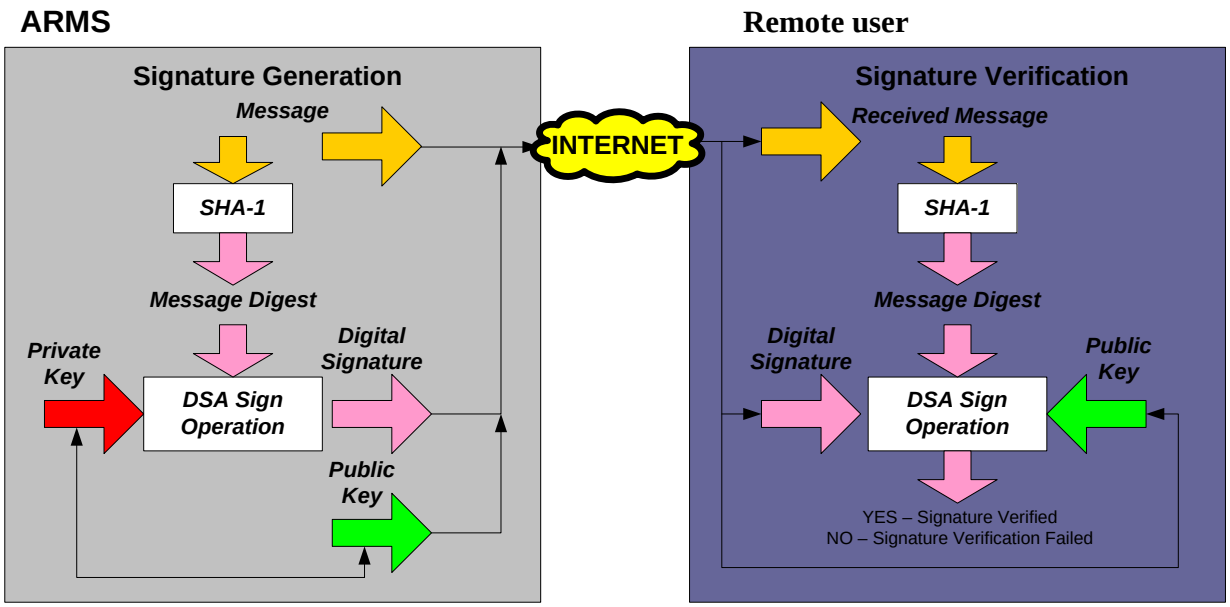

Figure 3: Authentication of data transmitted from the ARMS.

Data received by ARMS via RF, CAN, and an Ethernet interface from external devices and sensors are also subject to mandatory authentication using a digital signature with the Keyed-Hash Message Authentication Code (HMAC) algorithm. The principle of authentication of data transmitted to the ARMS is presented in Figure 4.

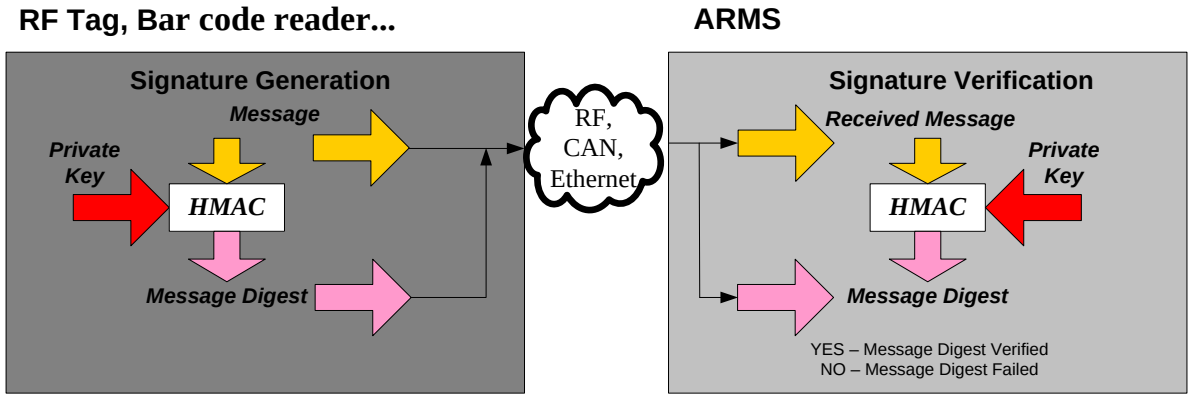

Figure 4: Authentication of data transmitted from external sensors

Events recorded by IR detectors, video cameras, RF tags, and the mobile barcode reader are complemented by a snapshot of the sector of the room where the access was recorded. The room is divided into four sectors according to the number of cameras. Each IR sensor and each video camera uniquely correspond to a certain area sector. Unlike IR sensors, RF tags monitoring containers with fissile materials may be located in any sector of the room. To integrate the system of RF tags into the ARMS, and to enable filming of container access event, a procedure of matching each RF tag with a corresponding sector must be performed. A similar procedure should be performed for external sensors and the mobile barcode reader. When the reader moves through several different zones, several zones may be listed.

The ARMS principles of operation are shown in Figure 5.

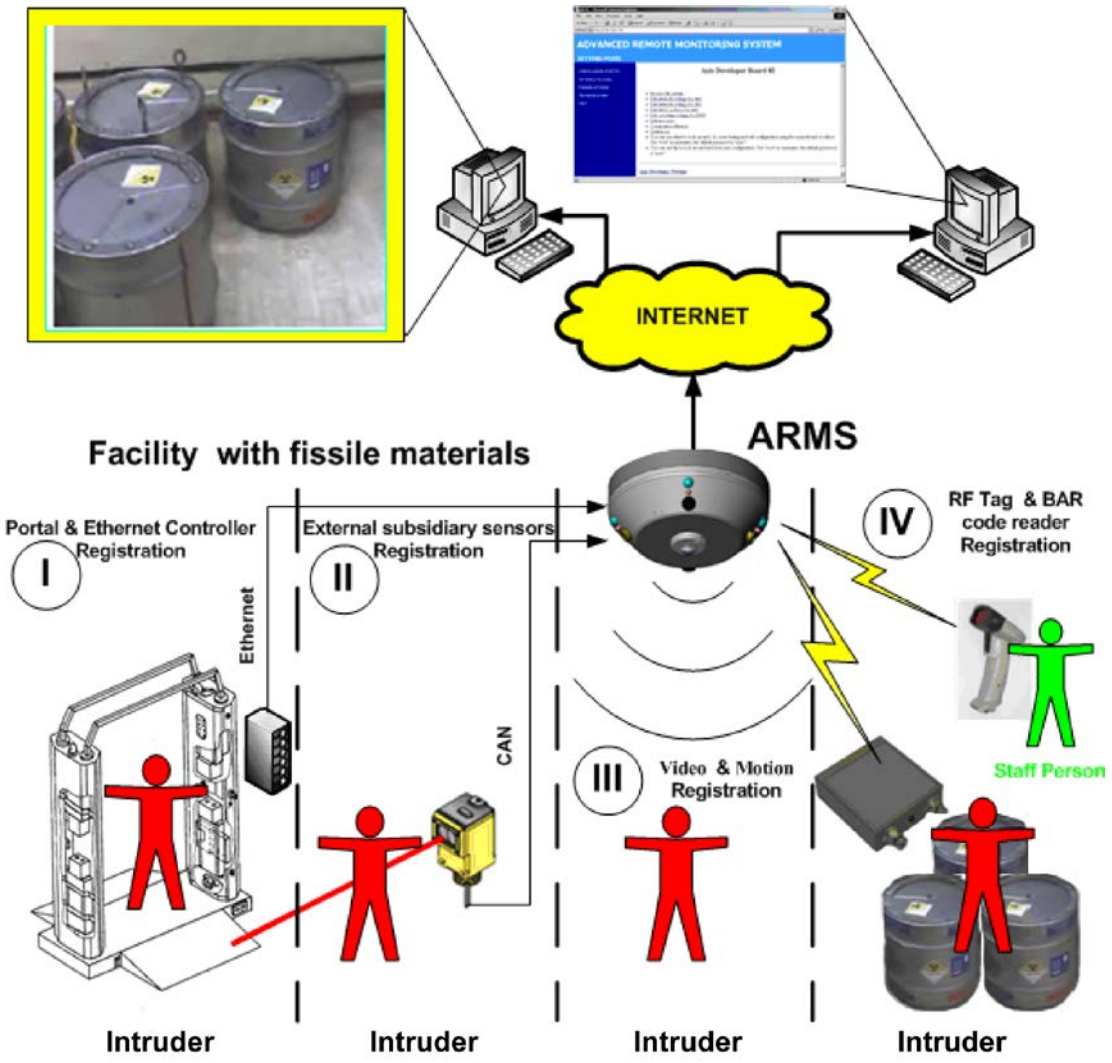

Figure 5: Principles of Operation

The event information stored in the database is presented in the form of a table on the Web page and contains the following data:

- Event type
- Alarmed sensor identifier
- Alarmed sensor state-of-health
- Event date and time
- Data authentication verification
- Picture of the area where sensors alarmed

To simplify the review and analysis, the information can be arranged by any data field. The user interface is shown in Figure 6.

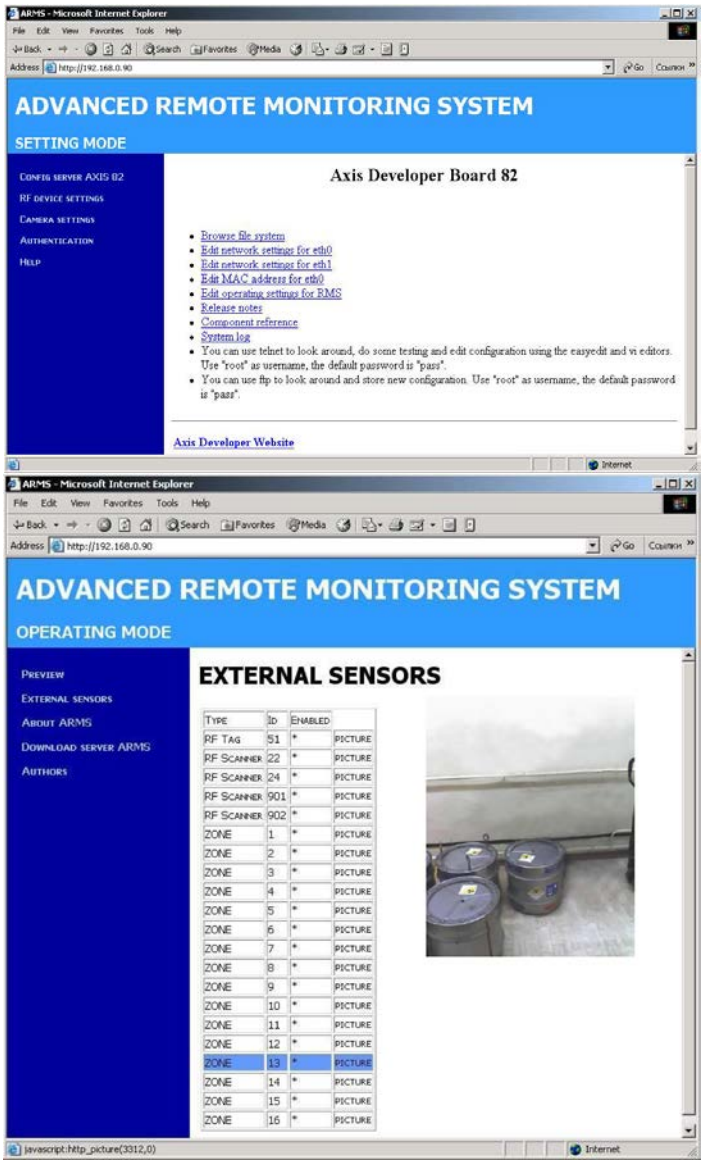

Figure 6: ARMS user interface

Conclusions

VNIIEF and SNL are currently engaged in researching, developing, and manufacturing ARMS prototypes. Plans are being made to conduct field testing of the ARMS in the F2F Demonstration storage facility at VNIIEF as well as at SNL.

The next stage will include development of external sensors supported by the CAN network with a built-in data authentication capability, and further development of ARMS for outdoor applications. These modifications will improve the quality of nuclear material storage monitoring and ARMS versatility.

Future plans call for ARMS to be IAEA-certified. Certification would allow us to expand the range of ARMS applications to include several Department of Energy (DOE) National Nuclear Security Administration (NNSA) programs, namely:

- Transfer of Russian-Produced Research Reactor Nuclear Fuel (RRRFR) Program — ARMS can be used for monitoring spent and fresh fuel in storage.
- Material Physical Protection, Control and Accounting (MPC&A) Program —ARMS can be utilized in material control and accounting systems to detect diversion of nuclear materials, and control unauthorized access and movement of nuclear materials.
- Cooperative Threat Reduction Program (CTR) — ARMS can be used in safe, secure, and environmentally sound storage facilities for nuclear material generated as a result of nuclear weapons dismantlement.