# F2F Storage Facility Monitoring System and Software Integration

Igor Bondar, Mikhail Osipov, Egor Terushev, Dmitry Pazhin,
Boris Barkanov, Anatoly Amelichev
All-Russian Scientific Research Institute of Experimental Physics (VNIIEF), Sarov, Russia

Lada Osokina, Troy Ross
Sandia National Laboratories, Albuquerque, New Mexico, USA

## Abstract

A storage facility with a total area of about 100 square meters was built with a purpose of testing both hardware and software components of the fissile material storage monitoring concept. This facility is divided into two rooms that simulate the actual vault and operator rooms. Both rooms house a number of equipment items intended for the storage facility monitoring application, including motion and break-beam sensors, radiation monitoring portal, radio frequency (RF) tags tracking container temperature and position, video cameras, and the first version of the Advanced Remote Monitoring System (ARMS). Data is collected and analyzed by unique software code.

This paper presents the principles that served as a basis for implementing software developed for the Facility-to-Facility (F2F) monitoring system at the Fissile Material Storage Monitoring Facility located in Sarov, Russia. The software ties together a complete system of collecting and assessing sensor events as well as obtaining images from video cameras connected to the system. The system is built as a client/server-type system. Data received from various modules/system clients is stored at the server in the MS SQL Server database. Currently, the system modules have been implemented as follows: control of video cameras via the TCP/IP protocol, operations with RF-tags used in the F2F system, and transmission of data via the Echelon bus or ARMS. The modules are networked to the server via the TCP/IP protocol, and the server ensures that all of the modules written into its configuration file stay connected.

In the process of the software design, special attention was given to the issue of reliable network communication between the modules and the server, and authenticity of data transmitted. The paper describes the data structure used for storing and displaying information on the F2F status, methods of improving reliability of the system functions, and a mechanism of getting images from video cameras without overworking the cameras or transmission channels, as well as a website structure that allows both assessment of the F2F status and system configuration.

## Introduction

As part of the Warhead Safety and Security Exchange (WSSX) Agreement Program, the All-Russian Research Institute of Experimental Physics (VNIIEF) and Sandia National Laboratories (SNL) have jointly engaged in the Facility-to-Facility (F2F) Project, which combines experimental systems for monitoring storage facilities in the Russian Federation and the United States, with the possibility of monitoring them via the global Internet network. Currently, the Russian experimental system is located at the Fissile Material Storage

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.

Monitoring Facility located at VNIIEF in Sarov, Russia. A SNL-developed experimental unattended monitoring system has been shipped to VNIIEF for installation and testing. Both systems contain commercially available equipment and equipment that the parties themselves developed to monitor the containers. This paper will describe the Russian system as developed and implemented for evaluation at the Fissile Material Storage Monitoring Facility in Sarov.

To perfect the mechanisms for monitoring the status of the storage facility, a model demonstration facility was created in Sarov in the form of a separate building with two rooms under contract with SNL. One room fully simulates a fissile material storage facility, with all the requisite attributes (see Figure 1). The second room is a simulated control room for the operators monitoring the status of the storage facility (see Figure 2).

All the equipment necessary for storage facility intrusion detection and status analysis is housed in the storage facility room: door sensors, motion detectors, and a portal radiation monitor. Installed on the simulated containers are radio frequency (RF) tags — developed by VNIIEF technical staff under contract to SNL — that monitor the temperature of the containers and verify that they have not been moved and that they remain sealed. The storage room has motion detectors, a door sensor, and break-beam sensors. An Echelon bus was originally used to connect all the sensors to the F2F storage facility monitoring system.

**Figure 1: Simulated Vault Area**

**Figure 2: Simulated Control Room with Operators' Workstations**

## Software Design

The software developed for the simulated storage facility is designed for acquiring, analyzing, performing various steps, and storing data from various types of security and information detectors. To enhance the functionality of the system, the system has a modular design and is based on client-server architecture. This makes it possible to expand the system with equipment based on various platforms for which modules have been produced. The ability to run each module on a separate computer makes it possible to decentralize the system, which can also enhance the reliability of its operation. To maintain data integrity at the proper level, the data transferred and stored are signed with a hash function, which makes it possible to confirm that the information has not been altered. Figure 3 gives a general diagram of the system's design.

The different information modules running on different computers are connected to the server. The server then authenticates the modules if required by the server configuration for a given module. If the authorization parameters are correct, the server registers the connecting module. After that, the server operates in waiting mode for information from the module on events involving the sensors for which it is responsible, or sends the module commands if it is an active-elements module. At the moment, there are two such modules in the system. One module was designed for operation involving the video cameras; the other was designed for operation involving the ARMS multifunctional electronic platform, which was also developed by VNIIEF technical staff under contract to SNL. In addition to operating in a waiting mode, the server periodically polls the modules to ascertain state of health to preclude blocking communication with the module, and blocking incoming information on sensor events. To expedite interactions between the system server and the database management system (DBMS), the server creates several connections and sets up a dynamic query queue, making them parallel in time. All the components of the system are multi-threading applications for the Windows operating system and take the form of system services. That will make it

possible to handle requests from several sensors independently. In addition, the use of multi-kernel processors or multi-processor platforms will profoundly enhance system performance without system modification.

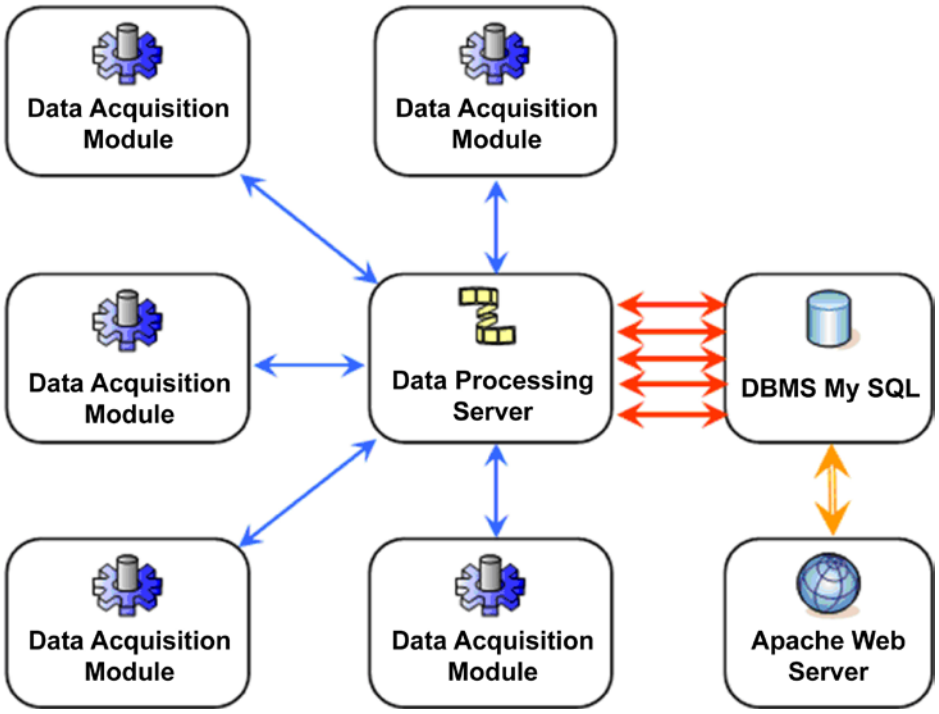


**Figure 3: General Block-Diagram of the System**

## F2F Monitoring System Description

For acquiring external data, the first version of the system employed the Echelon bus, which was used to produce an ample level of abstraction in the operation of different kinds of sensors, such as balanced magnetic switches, infrared motion detectors, and break-beam sensors. Nonetheless, in the second version of the system, when a dynamic "on the fly" reconfiguration of the system without direct access to the server became necessary, VNIIEF abandoned the version of the Echelon system because of its multiple-step operations for configuring the activity and availability of the sensors. At present, the F2F monitoring system can operate with video cameras that function with the HTTP protocol, and with a unit that interfaces with the RF tags and enables acquiring information from a large number of RF tags (tag loop breakage, tag movement, change in temperature or supply voltage). The F2F monitoring system can also send commands to the cameras and tags. An upgraded ARMS system is also installed into the monitoring system that supports the functioning of the motion sensors, pan-tilt camera, and RF tags base station.

The integrity of the data is achieved by employing a digital signature based on an HMAC algorithm. The module-to-server transfer of the data already involves the use of a signature, and that makes it possible to guarantee the integrity of the data when they are sent around the network. The server analyzes the signature and processes the data only if they are unaltered. If an error occurs while checking the signature, the server records that in the event log. The processing consists of entering the information into the database and polling the modules of the video cameras, which are configured as visual-information sources when a sensor records an event. In addition to the packet signature, the module of the video cameras inserts a data block into the file containing the JPEG image when transmitting to the server. This data block is the signature for the part of the file responsible for the image bitmap. When the server adds entries to the database that pertain to the status of the storage facility, the server signs each entry and attaches a unique identifier that automatically assumes the next consecutive number each time an entry is added. That makes it possible to ensure that entries have not been modified or deleted from the database, and that new entries have not been added. This process is accomplished in the following manner:

- an entry with an unfilled digital signature field is added to the database, and the information about the entry is not deleted from memory;
- the identifier of the most recently added entry is retrieved from the database, and the next consecutive identifier is assigned;
- that identifier is recorded to memory in its own location, and a digital signature for that block of memory is produced;
- an operation is performed for changing the field of the digital signature for the entry with that identifier.

To simplify the interaction between modules and server, there is a specific library (a dynamically loaded library, or DLL) that is designed to abstract the modules and the server from the data-transmission media. The library is built such that the modules and the server operate as if they were on the same computer and interact with each other via the standard Microsoft Windows mechanism-message exchange. All processes for connecting to the network, transmitting and receiving data, resending data in the event of transmission errors, and reconnecting to the network in the event of a break in the connection are transparent for applications — the library performs all the requisite operations in the background, with no need for the modules or the server to become involved. If connection cannot be made with the server, the library keeps all the information in memory until the connection is successful. If the connection cannot be made before the shutdown of the module service or the operating system as a whole, the library writes the information to disk and, during the next startup, loads it from the disk to memory, and sends it to its destination. Such an approach makes it possible not only to simplify the code of the modules and the server, but also to enhance reliability by reducing the overall size of the project code.

Analyzing the information acquired by the F2F system is done in two ways:

- the events that have occurred in the system over a time span are viewed with a WWW-interface
- the day-to-day acquisition of information on the status of the storage facility is done using the real-time events-acquisition module.

Figure 4 gives an example of a page that shows events registered by the F2F system.

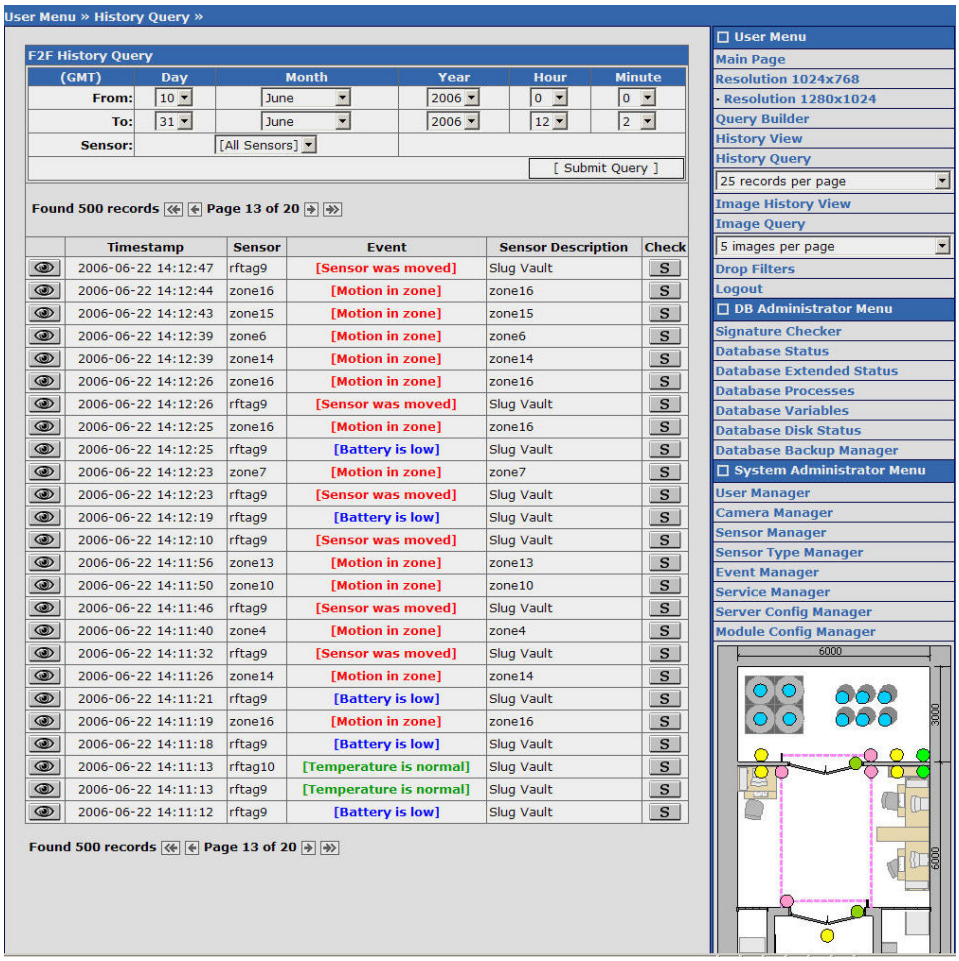


**Figure 4: Visual appearance of WWW-interface of F2F monitoring system**

The overall approach in the interface amounts to a dynamic menu that is assembled as a function of the currently registered user's privileges and the main dynamic portion located on the left side of the page, which reflects query result or menu function. The system supports three groups of users: the ordinary user, an analyst who is checking the status of the storage facility; the database administrator, who also has the right to perform operations involving system database management; and the system administrator, who has the right to perform the entire set of commands. Below the menu is an image of the simulated storage facility, with information pertaining to the location of the different sensors. When the cursor is placed on a sensor, the sensor name is displayed; when the user clicks on the sensor, a query is made requesting the display of the events associated with the sensor. In addition to the standard controls for paging through the query results, there may be two buttons on each line with an event — a button at the beginning of the record, and one at the end. A button with an image of an eye indicates there is a video image for that event; clicking on the button will display the set of photographs taken by the camera assigned for that event. The S button at the end of the

record allows for checking the authenticity of the record, i.e., the correctness of the digital signature for that record. When the photographs are being viewed, it is also possible to check a photograph's digital stamp. The WWW-interface scenarios interact directly with the DBMS server without affecting the system's efficiency to acquire and process the events.

Figure 5 shows the module for monitoring the status of the storage facility in real time.

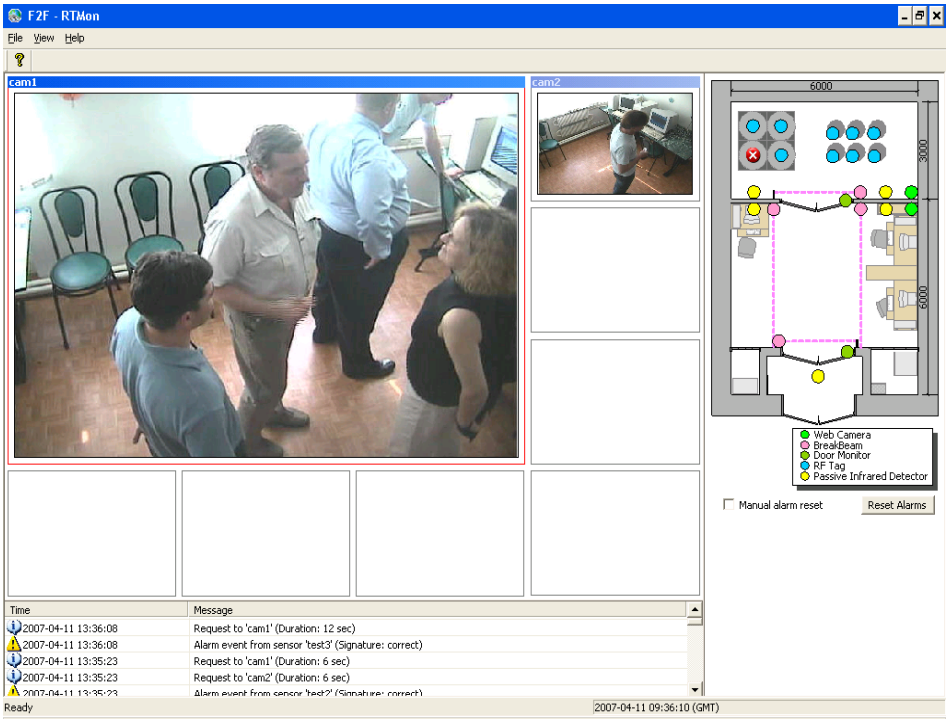


**Figure 5: Module for monitoring status of storage facility in real time**

The right side of the module ordinarily displays a plan view of the storage facility. A red circle may appear over the image of the sensor, as it does in this case, indicating the activation of that sensor. The main portion of the screen is occupied by a grid that is based on the number of configured cameras, whose images are cyclically updated for visual monitoring. The lower part of the window gives all the events that are being recorded by the system. When a sensor is activated (the lower left RF tag on the set of containers), the image from the camera assigned to that sensor enlarges, and an audible alarm attracts the operator's attention.

To enhance the reliability of the storage of information, there is a server and a client for data backup. That mechanism makes it possible to send information via the Internet, signing each transmitted block with a time key common to the server and the client. The server analyzes the information received and, if it has not been altered, saves it in a file. The client can then be used to restore it on another database server. The system server saves the information in a separate directory with the site name. This approach makes it possible to organize the centralized storage of information for various sites that use this monitoring system.

## Conclusions

The following steps may be considered in order to enhance an existing system:

- Changing the Echelon bus connection of sensors to a specialized Ethernet controller will enable dynamic configuration and acquisition of data with a digital signature
- Installing HTTP-controlled pan-tilt cameras will expand considerably the accessible field of the video surveillance and make it possible to show in greater detail the image of the area of a sensor whose status has been disturbed
- Introducing a messaging system (similar to a shift log) will enable operators to transmit information between shifts and users to raise questions
- Integrating new sensors and systems