SAND2010-3528C

APPLICATIONS OF NEXT GENERATION REMOTE MONITORING SYSTEM TECHNOLOGIES (NGRMS)

Barry D. Schoeneman
Sandia National Laboratories
bdschoe@sandia.gov

Abstract

This paper discusses application scenarios for Next Generation Remote Monitoring System (NGRMS) technologies and how data resulting from these applications may be utilized. These technologies are primarily designed for two application regimes: Treaty Verification and Nuclear Safeguards. The NGRMS technologies provide for active monitoring of important items and environments. These are greatly beneficial for applications where it is required that the information provided maintains high levels of information confidentiality, verification of source and a high degree of confidence in the security of the devices deployed. This paper provides a view of how these technologies can be deployed and how their data can be utilized for the application scenarios discussed and why certain capabilities are important for successful monitoring system implementation. The advantages of a common communication protocol for both wired and wireless transmissions, autonomous operation, information sign-store and forward as well as world-wide access to the sensor information are presented.

Introduction

The focus of this paper will deal with the application of monitoring technologies, as components of a monitoring system that have been, or are being, developed under the NGRMS Program for the Department of Energy, Office of Nuclear Nonproliferation by Sandia National Laboratories' International Safeguards and Nuclear Monitoring Science & Technology Department. Some of the applications scenarios are hypothetical, but are based upon design capabilities that will be realized within the near future.

To detect undeclared diversion of nuclear materials, advanced sealing and monitoring system technologies are required as an integral part of any containment surveillance (CS) approach. As adversarial capabilities continue to advance, so must the challenges presented to an adversary with the expressed purpose of preventing the adversary from succeeding in their goal - circumvent the monitoring system and gain undetected access to monitored items. The intelligent integration of security concepts into a physical technology used to monitor items is a fundamental requirement for secure containment and surveillance. It is recognized that monitoring technologies are only part of the CS solution, but they play a very important role in surveillance. Seals and sensors[i] (referred to as sensors from this point forward) represent a broad range of complexity and capability. The application environment will ultimately determine how sensors are utilized. Currently available technologies fall seriously short in the ability to provide the high confidence of detection, high confidence in collected information, confidentiality, and timely notification that can be appreciated with new technology. The seals and sensors developed for the NGRMS program currently provide these capabilities as a foundation. The NGRMS program has allowed the integration of these concepts, from the ground up, without compromise. The end result is a purposely designed suite of seals and sensors for monitoring systems. Additionally, as monitoring needs rapidly expand, out pacing budgets, remote monitoring of low-cost autonomous monitoring technologies becomes increasingly appealing. The Remotely Monitored Sealing Array (RMSA) utilizes this technology and has implemented cost effective security concepts establishing the high confidence that is expected of active sealing technology today.

1. Application environment

The sensors that have been developed under the NGRMS Program are a set of monitoring tools that incorporate sensible, cost effect security, long term autonomous operation, and low life-cycle costs resulting in high confidence information. In this context, the confidence in the information provided by these tools is established by a common theme and approach for the generation and initial processing of information, to be done at its origin, in a secure[ii] environment. Once sensor data is captured in this environment, time variants are added, it is passed through cryptographic functions and then it is stored and transmitted. The secure environment protects keys and other sensitive information with tamper features. Some of these tamper features are active and some are passive, or intrinsic to the housing, design. The combination of these security based fundamental features make this set of tools well suited for treaty verification and nuclear safeguards applications.

1.1. Treaty verification Regime

Weapons related items and materials are typically are the focus of treaties between nuclear weapons states. This represents a wide spectrum of items from launch vehicles to lose nuclear materials that could fall under the monitoring agreements of a treaty. One concept that is discussed for treaty verification is chain of custody (COC). The general theory of COC is to maintain the identity of a monitored item and it components throughout its life cycle as dictated by the treaty. Sealing monitored items performs two functions: an appropriately applied seal can uniquely identify items through association with the seal's unique identification and it can detect if the item has been altered. A seal is only one component of a system that monitors the integrity of the monitored item's containment and the success of the system is dependent upon the integration of all of the components. Other NGRMS sensors that are or can be available that can be applied in a treaty verification regime are: the gamma-ray spectrometer which can be used to determine if material is present and whether substitutions of the monitored material have occurred; sub-nanometer surface feature extraction (SSFE) which can uniquely identify an item by continuously verifying a 2.5mm^2 surface area; and the authenticated magnetic switch for monitoring doors or providing authenticated triggers to other devices, such as a camera.

1.2. Nuclear Safeguards

Nuclear safeguards are applied to processes and material associated with the nuclear fuel cycle. Typically monitoring is performed in all phases of the fuel cycle including interim storage before final disposition. This can include internment and re-processing. Essentially anytime the material is attractive for diversion it can be monitored under safeguards agreements. As the nuclear renaissance approaches monitoring technologies, such as the NGRMS ones, are going to play a greater role in the solutions sought for effect nuclear safeguards oversight. 'More with less' is going to be the 'Theme Dejour'.

Remote monitoring as well as remote inspection will be routine in the near future. The NGRMS monitoring technologies have been designed as tools to support this looming need. These monitoring technologies provide remote access to the translator as well as each individual sensor. Figure 1 depicts the configuration of a monitoring system that can provide remote access to many RF and hardwire sensors. The remote access capabilities of this system include direct access to the translator (may be through an intervening device such as a virtual private network [VPN]) and indirect access to individual sensors from the data review station. The purpose of allowing access to individual sensors is to recover missed messages and/or request the state-of-health (SOH).

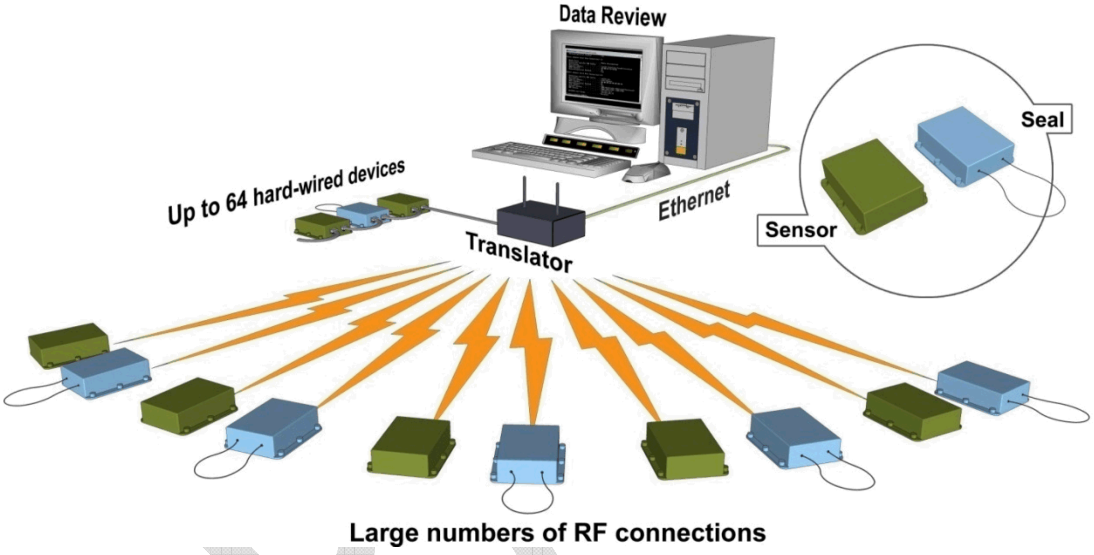

Figure 1 Typical Sensor and Seal Configuration with Remote Access

2. Information Utilization

The NGRMS sensors generate information that can have a variety of uses. Three of these are:

- Security,
- Conclusions, and
- Triggering.

Because the NGRMS sensors transmit immediate alert notification, they can be utilized as an integral part of a security system. An example could be the use of a fiber optic seal to monitor special nuclear material (SNM) in a storage facility. If a fiber break is detected the monitoring system is notified immediately by the seal and a security response can be initiated. Augmenting an existing security system with such sensors can provide justification to extend physical inventory taking (PIV) requirements for SNM storage facilities. As a security system component, it may not be necessary to perform both authentication and encryption to conceal and authenticate transmitted information. This is especially true if only one party is utilizing the information. Encryption only can satisfy both requirements to conceal and authenticate information in this situation.

Utilizing information collect from sensors of this type can also be utilized to form conclusions about the monitored item and its recent past. This type of application does not require immediate notification such as is required of a component of a security system. However, the provisions for the collection and handling of this information must establish the highest level of confidence possible. This is why authentication and encryption are such an important capability for embedded sensors that are used in either nuclear safeguards or treaty verification where determining the status of a monitored item is used to draw conclusions. The source of the information must be known, absolutely and the fact that it has not been modified must be established, without question.

A trigger is greatly useful when it is desirable to collect substantiating information based upon an associated event. A door switch state change event can be used to generate a trigger that causes the camera to capture images of the circumstances that caused the door event. The problem with this sequence is that the trigger could easily be counterfeit. There are a number of reasons that this is a suboptimal situation, but this is not the subject of this paper. The NGRMS sensors can provide authenticated trigger messages between two associated sensors, addressing the counterfeiting issue. A door switch can send a signed message to a camera connected to a trigger module and once the message source has been verified, the camera will be triggered. Figure 2 depicts a hypothetical system configuration utilizing a door switch to send an authenticated trigger message to an associated surveillance camera. In this case the camera would only perform its trigger function when a message is verified. Authenticated triggering does not preclude other camera functions. This capability is especially useful when RF communications are used and these sensor pairs can be deployed in a virtually ad-hoc[iii] manner for a given application environment.

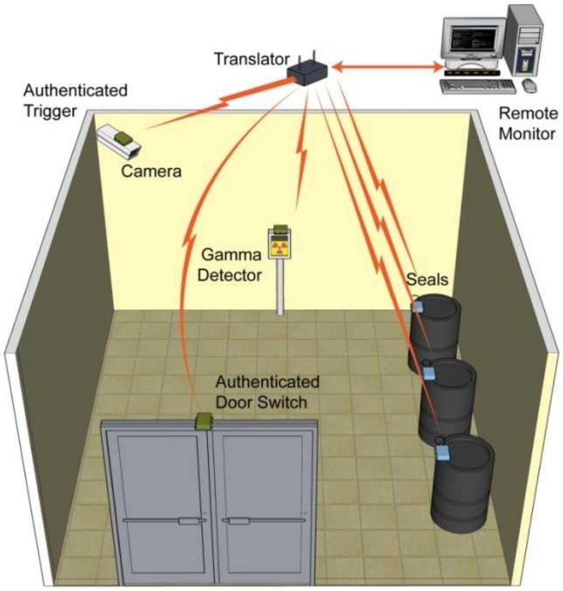

Figure 2 Hypothetical Use of Authenticated Triggering

2.1. Joint Use

Confirmation of a monitoring agency’s safeguards conclusions can be based upon jointly verifiable information derived from a combination of inspectorate owned equipment and shared (jointly monitored) equipment. Currently, the jointly monitored equipment provides supplemental information which can be used to further substantiate safeguards conclusions. Eventually, as the quantity of operator owned equipment used to provide this supplemental data increases, the implied effect will be to significantly increase the difficulty for viable material diversion paths and to reduce operating cost to the inspectorate. The only way to generate jointly verifiable information from NGRMS sensors is to use an asymmetric key configuration for authentication and share the public part of the key with the verifying parties. The primary verifier (likely the inspectorate) would load the secret part of the authentication key pair into the sensor before deployment in a secure environment. Encryption is a different situation in a joint use application model because the information is encrypted for confidentiality purposes. For example, encryption would be used protect information that may reveal a proprietary process. Collected information can be decrypted by the inspectorate and provided to the operator for verification, if desired. The encryption/decryption process is not as sensitive to the inspectorate as is the authentication process. Because this information is used to draw safeguards conclusions, its authenticity is critical.

2.2. Single Use

Information used to establish safeguards conclusions are not shared and the equipment used to acquire data are owned and maintained by the inspecting agency. For this type of application the data from NGRMS sensors can be authenticated and encrypted using either a symmetric (private) key pair or asymmetric (public) keys. The advantages to using the asymmetric key pair for authentication is reduced key management related overhead and security implications result from key exposure. The public part of the key pair can be revealed without compromising the security of the signing key. Keys can be carried into the field, if need be, for information verification. Currently, the NGRMS sensors only support the asymmetric key configuration for authentication by the addition of a public key crypto-processor (PK processor). Therefore, utilizing these sensors for single use scenarios will require the use of cryptographic keys in either of two configurations:

- Symmetric keys for authentication and encryption, or
- Asymmetric keys for authentication and symmetric keys for encryption.

It also needs to be made clear that the NGRMS sensors equipped with the PK processor do not provide a "public key infrastructure" for a system utilizing this option. The PK processor does provide signatures for transmitted information based upon this process; however, the user must provide the infrastructure (e.g., certifying authority).

3. Security

Embedded sensors such as the ones developed by the NGRMS Program must strike a balance between unit cost and security features. The NGRMS suite of sensors has utilized the expertise of vulnerability assessment (VA) specialists during the design of these sensors to perform periodic 'vulnerability reviews' with the desired outcome of mitigating issues that would be identified during the formal VA process that any sensor would endure before being accept for routine use in any monitoring regime. Not only did this process identify design course corrections, but it allowed the integration of a security based design philosophy from the beginning. The results of this can be especially appreciated in the communication protocol. The end result is a framework of security based capabilities which protect the confidence of collected and transmitted information from its creation within a secure, tamper indicating housing to the review software where the information is utilized. The NGRMS sensors are not perfect in this pursuit, however, they are the best implementation for the cost. Information that cannot be verified cannot be utilized for safeguards or other critical conclusions, period.

3.1. Information

There are several methods utilized by the NGRMS sensors to protect the integrity of the information that is collected and transmitted. Cryptographic keys are destroyed upon user selectable tamper events as well as managed with 'low-persistence' algorithms. These keys are loaded into the sensor in a secure environment prior to deployment and are actively protected throughout deployment. Messages to be transmitted include time variants and unique identifiers to virtually eliminate the possibility of an authentication collision[iv]. Another important requirement for overall confidence in information generated by these sensors is to provide complete data sets. The collected information must form complete sets of data. Any gaps will cast doubts about the conditions of collection. Therefore, NGRMS sensors incorporate the concept of 'sign, store and forward' (SS&F). This theme provides redundant information repositories to assure, with a high degree of confidence, that complete sets of information can be established. SS&F is implemented at the sensor level and again at the data collection point (translator) in nonvolatile memory with enough space to store years worth of messages (encrypted if this feature is enabled) under normal circumstances[v]. Based upon this capability, an individual message can be recovered from an individual sensor, or the data collector, upon request from the user system years later. At the time of this paper, NGRMS sensors use 128 bit AES for authentication and encryption functions. Another information security feature of this family of sensors is that all NGRMS sensors are programmed with a reporting interval for autonomous 'state-of-health' (SOH) messages. The intent for this feature is to provide the user with dependable, predetermined reports of each sensors operating status. The obvious use of this information is to monitor the health of a sensor and the environment is which it is operating. The other less obvious use is to detect anomalies in the operating environment which may indicate a change, intended or unintended, in the sensors communication that may require further investigation. Additionally, a number of programmable events can be selected to initiate immediate transmission of alert messages in addition to the periodic SOH reports.

3.2. Hardware

There are three fundamental types of hardware security utilized in the NGRMS sensors. They are:

- Active,
- Indicative, and
- Passive.

For any application it is important to realize that hardware security features require some supplemental external processes to be completely effective. Active tamper detection is the least reliant upon external process. A detect tamper occurs and the remediating action is taken. For instance, a case tamper is detected by the MCU (micro-controller unit) and sensitive information is destroyed (e.g., cryptographic keys). For this type of remediating action, the correct events need to be selected so that information is not destroyed prematurely or not at all. The select must be made carefully and with respect for the application environment. Indicative features are one that are intrinsic to the sensor and are typically examined and evaluated through some external process. When considering the implications of indicative security features it is important to realize the external processes that will be needed to fully utilize their usefulness. The incorporated indicative features of the sensor package will need to be inspected and documented prior to deployment, as well as in the field and forensically to 'perceive the signs' and determine if tampering has occurred during its deployment. Some new technologies that are available to support inspection and documentation of indicative features are flash thermography and reflective particle tagging. Supplement processes like this are an important requirement of hardware security that is often overlooked or simply not implemented. The passive security concept is one which is inherent to the hardware design and causes either an active or indicative feature to be triggered as a result of violating the secure housing. When combined and appropriately supported these three security methods are highly effective.

4. NGRMS Sensor and Sealing Technologies

The NGRMS program at Sandia National Laboratories has developed several sensor and sealing technologies, some are currently available for production, some are in the prototype phase and some are still concepts. All of these technologies utilize the Secure Sensor Platform (SSP) framework of capabilities. As shown in Figure 3, the SSP framework allows sensors to inherit all of the core capabilities establishing a common operating protocol. Any sensor based upon this framework can readily co-operate within an SSP based communication environment. A SSP gamma detector can be added to a deployed seal monitoring system without issue.

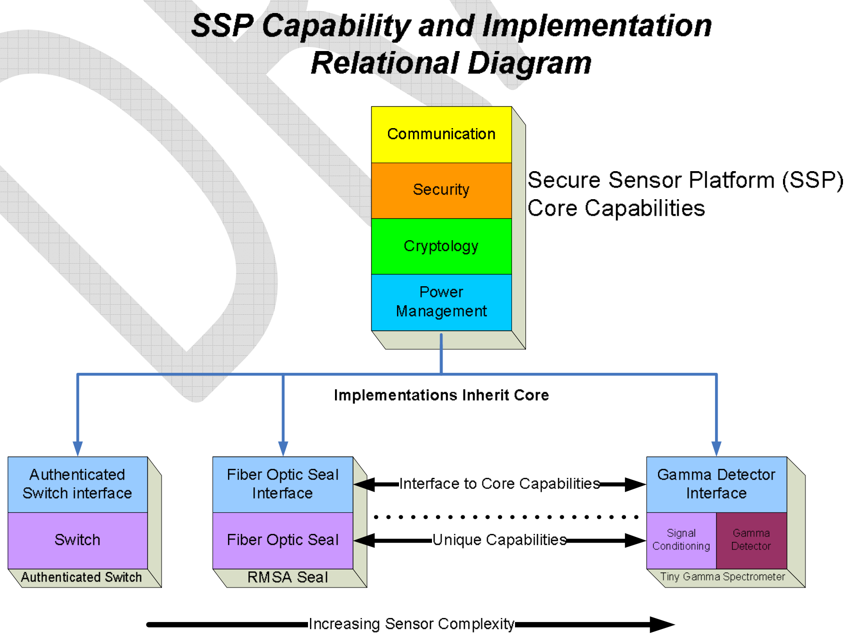

Figure 3 Secure Sensor Platform (SSP) Framework Inheritance Diagram

At a more detailed level, the common operating protocol also extends to the sensor’s memory management with sign, store and forward (SS&F) implemented in all devices. Similarly, autonomous operation and remote access are common throughout all platforms. Each sensor design, however, is application specific at the interface between the SSP framework and the actual sensor to be monitored. This is called the ‘interface to core capabilities’ and this is why each sensor implementation is unique and requires its own specific design. This uniqueness includes software drivers, electronics, and typically a new housing design.

Currently, a fiber optic seal is available for production along with an ultra short range handheld reader and all of the supporting system components for local and remote access. These seals communicate using unlicensed RF and are battery powered. The handheld reader is intended to be used to confirm seal (or any SSP RF sensor) operation at installation and also randomly during deployment. Its primary purpose is to authenticate, through a ‘challenge response sequence’ the seal’s identification and provide a rollup of its current operating status. Nearing completion is an authenticated switch and trigger unit for possible application as a source for triggering cameras. Another supplemental device in this phase is the public key processor. This device adds a public key signing capability to any SSP based sensor design. In the prototype phase is a tiny gamma-ray spectrometer (TGS). This is an ultra low-power gamma spectrometer. The TGS does this by sleeping most of its deployment life, waking periodically based upon some internal trigger, and captures a gamma energy spectrum of the current environment.

[i] For practical purposes an active seal is a sensor. In this paper seals and sensors will be generalized as sensors when referenced collectively.

[ii] The term ‘secure’ is relative. Cost it an important constraint to the development of secure environments for embedded sensors. The monitoring tools discussed here are intended to be cost effect solutions that can be widely deployed. Security was a core competency required for the development of these tools, offering the best security implementation possible for the cost. Cost benefits have been maximized.

[iii] Within the constraints of the RF capabilities or the RS-485 capabilities should hardwire be used.

[iv] An authentication collision results when two different but sensible, cryptographically signed, messages have the same signature. It is immensely difficult for this situation to occur when message protocols incorporate time variable fields and a strict message structure are used.

[v] Normal conditions would be two SOH message transmissions per day, which is typical for providing timely status information.