Ultra Secure High Reliability Wireless Radiation Monitor

Joseph V. Cordaro, Davis Shull, Mark Farrar, George Reeves
Savannah River National Laboratory
David Aylesworth, Fortress Technologies Inc., a subsidiary of General Dynamics

Introduction

Radiation monitoring in nuclear facilities is essential to safe operation of the equipment as well as protecting personnel. In specific, typical air monitoring of radioactive gases or particulate involves complex systems of valves, pumps, piping and electronics. The challenge is to measure a representative sample in areas that are radioactively contaminated. Running cables and piping to these locations is very expensive due to the containment requirements. Penetration into and out of an airborne or containment area is complex and costly. The process rooms are built with thick rebar-enforced concrete walls with glove box containment chambers inside. Figure 1 shows high temperature radiation resistance cabling entering the top of a typical glove box.

Figure 1: Typical Glove Box Wiring at a Nuclear Facility

In some case, the entire processing area must be contained in a “hot cell” where the only access into the chamber is via manipulators. An example is shown in Figure 2.

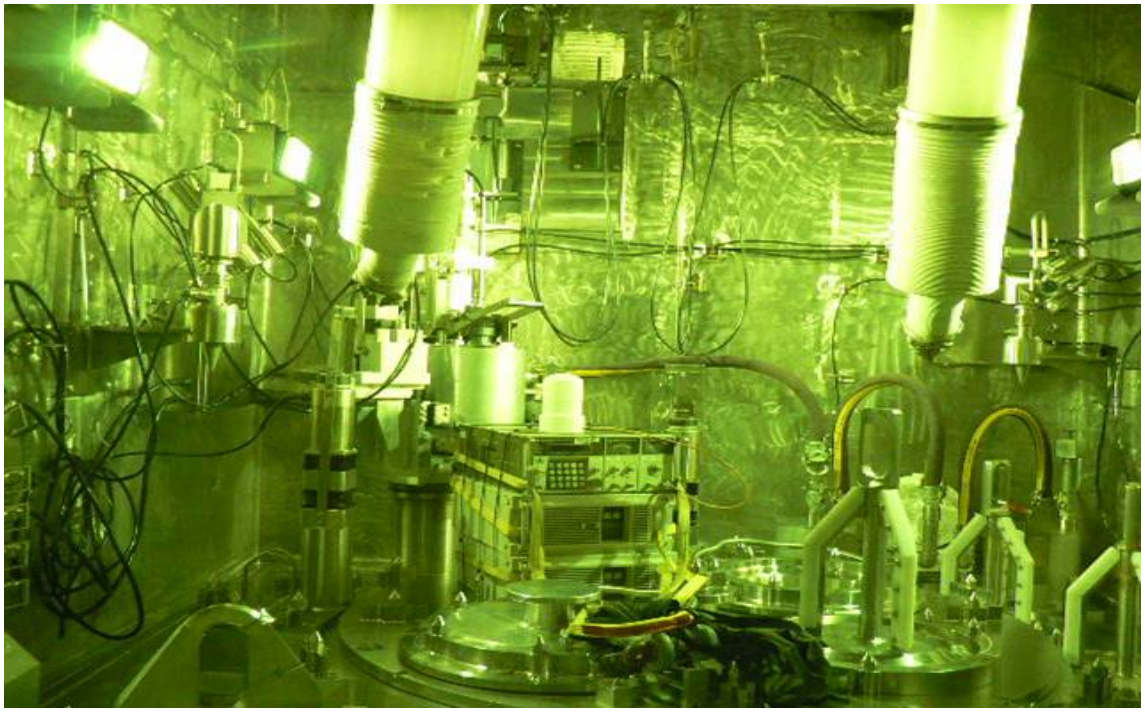

Figure 2: Hot Cell at the Savannah River Site

A short range wireless network provides an ideal communication link for transmitting the data from the radiation sensor to a "clean area", or area absent of any radiation fields or radioactive contamination. Radiation monitoring systems that protect personnel and equipment must meet stringent codes and standards due to the consequences of failure. At first glance a wired system would seem more desirable. Concerns with wireless communication include latency, jamming, spoofing, man in the middle attacks, and hacking.

The Department of Energy's Savannah River National Laboratory (SRNL) has developed a prototype wireless radiation air monitoring system that address many of the concerns with wireless and allows quick deployment in radiation and contamination areas. It is stand alone and only requires a standard 120 VAC, 60 Hz power source. It is designed to be mounted or portable. The wireless link uses a National Security Agency (NSA) Suite B compliant wireless network from Fortress Technologies that is considered robust enough to be used for classified data transmission in place of NSA Type 1 devices.

Background

Existing air monitoring systems depend on an array of piping into the process rooms for sampling the environment. Monitors are located in clean areas and a system of pumps and valves are used to draw an air sample into a radiation detector. Limit switches are required on the valves to ensure they are in the open or closed state and flow switches are required to ensure a representative air sample is drawn into the detector. A PLC or

similar control system continuously cycles the valves such that each monitoring point is sampled at the required interval to ensure safety of personnel.

An ion chamber is typically used to measure the airborne radiation. Figure 3 shows the basic design of an ion chamber.

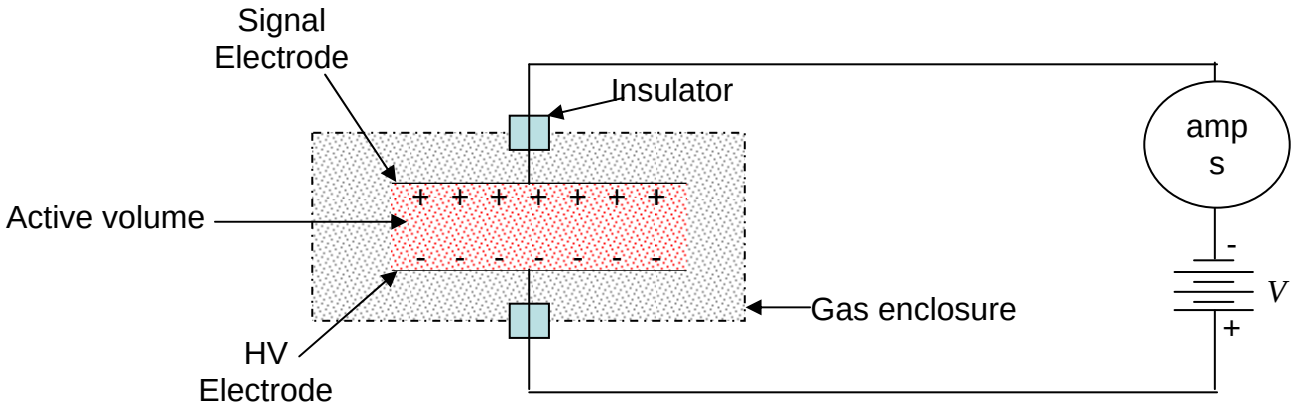

Figure 3: Diagram of an Ion Chamber and Electronics

High voltage is applied to the HV electrode such that the radioactive gas will be ionized generating a very small current that is measured by an electrometer. Background currents can be as low as 10 Femto Amps (i.e. 1.0E-14 A). Since false alarms will cause major facility disruptions, the ion chamber electronics must be able to measure these currents without generating false trips even in the presence of electromagnetic interference generated from solenoids, pumps, variable speed drives, etc.

Radiation Sensor and Electronics

Building upon an electrometer design with a patent pending (reference 2), SRNL developed an ion chamber that allows radioactive gas to pass between the cylindrical screens. The plate spacing has been designed such that the operating voltage is 50 Volts eliminating electrical safety concerns over the exposed energized screen. The outer screen, however, is grounded. Figure 4 shows an example of a screen wire chamber.

Figure 4: Screen Wire Ion Chamber

The ion chamber is a coaxial design consisting of three concentric cylinders. Each cylinder is an electrode fabricated of stainless steel screen. Voltage is applied to the middle electrode. The outer electrode is grounded and acts as an ion trap for ions that have been generated outside of the active volume of the chamber. The volume between the center electrode and middle electrode defines the active volume. All ions generated within that volume are swept to the center electrode generating a small current, typically in the range of 1.0E-14 to 1.0E-3 amps.

Typically, ion chambers are designed to operate at a bias of several hundred volts to ensure complete collection of the ions generated. Because this chamber would be operated in areas accessible to personnel, the chamber was designed to operate at 50 VDC. A saturation curve was generated with the ion chamber immersed in a gas chamber. As shown in Figure 5, the chamber reaches 99% of the saturation current at 25 VDC and is stable to within 1% of reading over the range of 40 – 60 VDC. Leakage current is problematic with the currents at which these devices operate. Therefore, great care is taken during fabrication to maintain the cleanliness of the electrodes and insulators. Once in the field, the chamber will, over time, collect dust resulting in abnormally high and fluctuating background measurements. In order to alleviate this issue, a sheet of 5 micron filter paper is fixed around the chamber and periodically replaced in the field. The 5 micron filter paper protects the ion chamber from dust and other contaminants but does not measurably change the instrument response time.

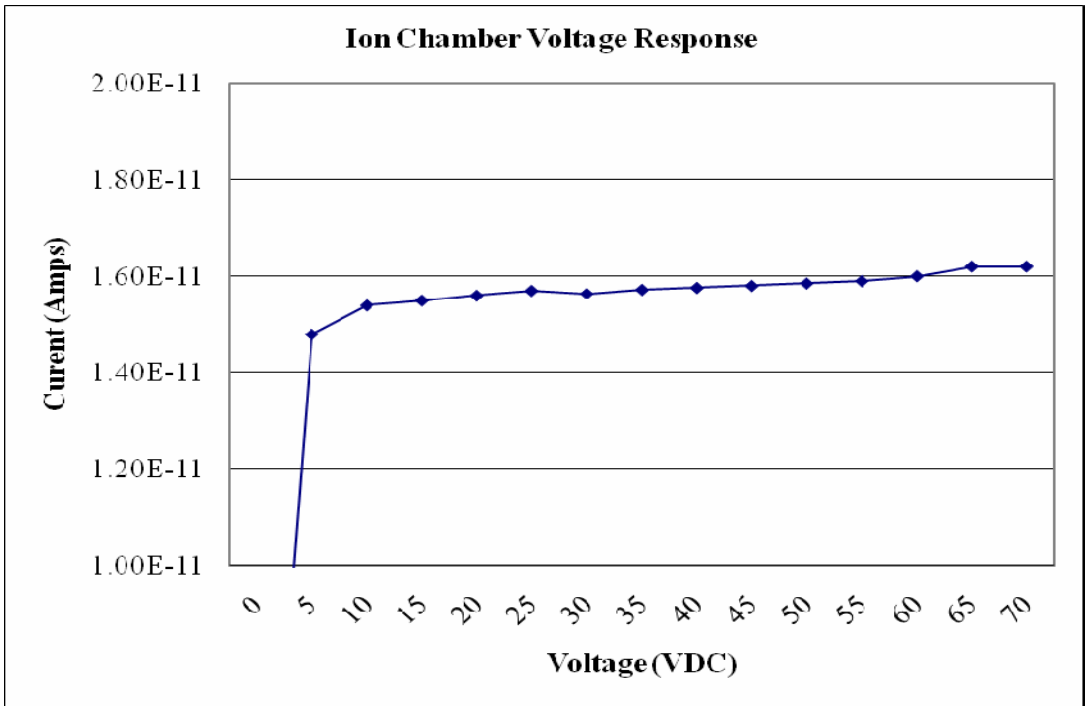

Figure 5: Saturation Curve for Ion Chamber

Calibration is performed using National Institute of Standards and Technology (NIST) traceable gas mixture in a sealed chamber at multiple concentrations. The calibration uncertainty was approximately 7% of reading, 2 sigma, with the primary contributors being the uncertainty of the NIST standard itself and the random uncertainty of the measurement.

Since nuclear facilities utilize high flow HVAC systems that are designed to move air quickly from the clean area into process areas then to a stripper or similar system, diffusion is sufficient to get a representative air sample into the screen wire chamber. The sensitivity of the ion chamber is determined by the active volume and background current of the electrometer. Active volume can be increased, increasing the sensitivity; however space and weight become a limiting factor. Utilizing an electrometer design that can measure 1 Femto amp in the presence of EMI, allows for a fast response to any airborne activity above normal background. A custom pre-amplifier has been developed (reference 2) with a multi-layer printed circuit board located in a radio-frequency and magnetic field shielded enclosure. A top view of the enclosure is shown in Figure 6.

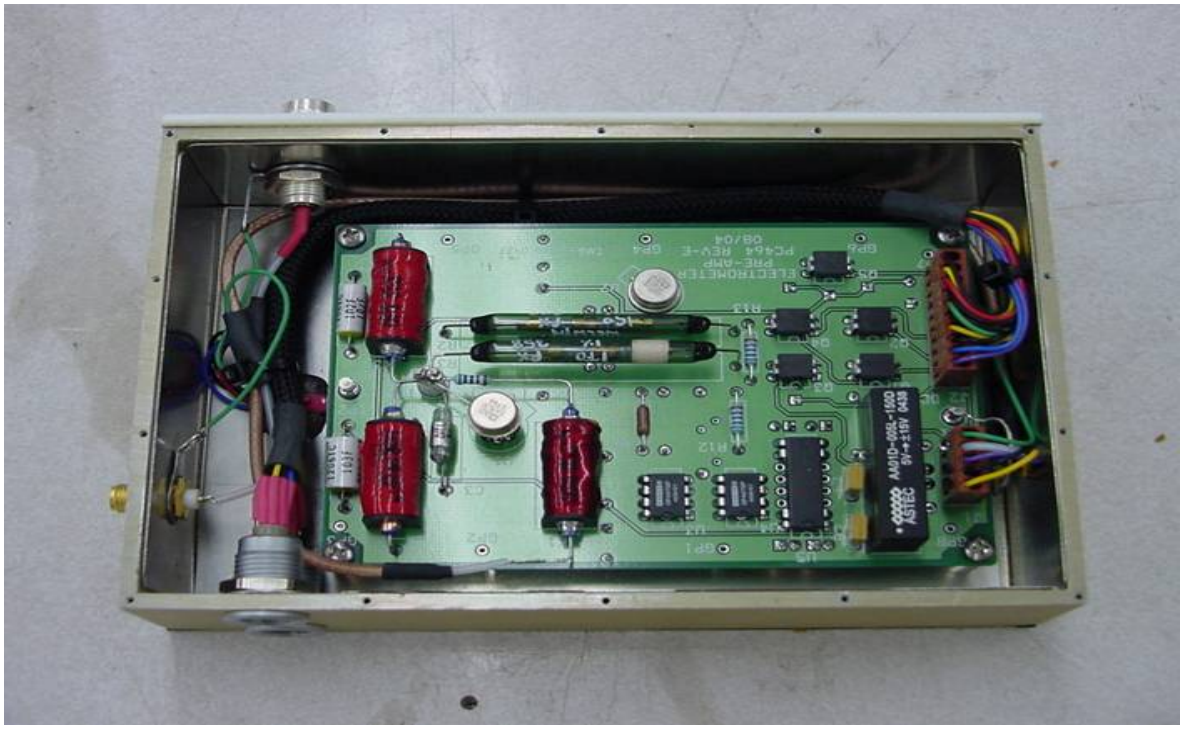

Figure 6: Ion Chamber Pre-Amp Electronics

The pre-amp features a 1st stage gain of 1 Trillion. The 1st stage amplifier has a 60 Femto Amp input bias current. The 2nd stage has a gain of 100, but it is combined with a temperature compensation circuit that corrects for the offset of the 1st stage amplifier. Mu metal was used to line the interior of the RF enclosure to minimize magnetic fields as well as electrical fields. This was essential to minimizing the background current to a few Femto amps. The single-pole-single-throw relays have three leads, two for the relay

signal and one that connects a faraday shield around the relay to the ground plane in the printed circuit board. A PC104 single board computer is used to monitor the output of the pre-amp voltage to trigger range changing relays such that the pre-amp can measure from Femto Amps to Micro Amps. The PC104 software, written in C code converts the current to engineering units such as micro curies per cc. The PC 104 computer has a RS232 serial output for transmitting the activity data, alarms and system status.

Wireless Network

A wireless network provides several advantages over the typical wired monitoring systems. The cost of running cable into a process room can be as high as $2000 per foot. A wireless system could save $ per deployment. In addition, the sensors can be placed anywhere, removing the need to pump air samples to the sensors. By removing certain components from the system, it is expected that wireless air monitoring will actually prove to be more reliable than the wired equivalent. Security issues can be mitigated by a combination of cryptography.

Classified government communications are protected by special “Type 1” encryption products that are controlled by the National Security Agency (NSA). In order to prevent these products from falling into the wrong hands, they have strict security controls that make them cumbersome to store, operate, and share with partners. These products also take multiple years to design and develop, and the lengthy process doesn’t allow products to keep pace with technology innovation. Since these products are only sold to the U.S. government, which limits the market size, the resulting products are significantly more expensive than commercial alternatives that solve similar problems. With the development of more mature and robust open standards, the NSA is addressing these issues through “Suite B Cryptography” (reference 4), a set of approved commercial algorithms and protocols that, when implemented correctly in a layered approach, can be used to protect classified U.S. government information up to the SECRET level. Suite B has been selected by the NSA from cryptography that has been approved by NIST for use by the U. S. Government and is specified in NIST standards and recommendations.

Suite B is part of the NSA Cryptographic Interoperability Strategy (CIS), developed to improve information sharing within the U.S. and with coalition partners. Open standards and the use of strong public algorithms provide interoperability and allow for the possibility of release to coalition partners or state and local governments. Suite B may be used to protect sensitive but unclassified (SBU), as well as classified information (SECRET) with NSA approval, where currently only Type-1 products are approved. This provides a solution that will free organizations from the onerous burdens and handling requirements currently associated with Controlled Cryptographic Item (CCI) equipment. Since the vast majority of classified information is SECRET or below, approved Suite B products could significantly improve the speed and flexibility of deploying secure, COTS-based communications systems. Table 1 details the algorithms associated with Suite B. . In addition to implementing the proper cryptographic protocols and algorithms, these Information Assurance Suite B products must be validated and certified

in accordance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Revised Fact Sheet National Information Assurance Acquisition Policy (reference 5). Depending on the information being processed, this validation and certification must include NIST Federal Information Processing Standard (FIPS) certification under the Cryptographic Module Validation Program per FIPS 140-2 Security Requirements for Cryptographic Modules and evaluation per the NSA/NIST National Information Assurance Partnership (NIAP) evaluation and validation program. In addition, Suite B products intended for use on classified systems must undergo additional evaluation by the NSA.

Confidentiality (Encryption)	Advanced Encryption Standard (AES) FIPS PUB 197 (using key sizes of 128 and 256 bits)
Integrity (Hashing)	Secure Hash Algorithm (SHA) FIPS PUB 180-3 (using SHA-256 and SHA-384)
Key Exchange / Establishment	Elliptic Curve Diffie Hellman (ECDH) NIST Special Publication 800-56A (using 256 and 384-bit prime moduli curves)
Authentication (Digital Signature)	Elliptic Curve Digital Signature Algorithm (ECDSA) FIPS PUB 186-3 (using 256 and 384-bit prime moduli curves)

Table 1: Suite B Algorithms

In order to meet the commercial standards-based layered solution requirements for using Suite B, a wireless sensor network based on the IEEE 802.11 WLAN standards was chosen. The maturity of the 802.11 security protocols was a key influencing factor in this selection. Fortress Technologies was awarded the contract to develop this 802.11 wireless sensor network solution for the Department of Energy based on their leadership as an early adopter of the NSA's Suite B vision. Using existing components in the Fortress product line enabled the rapid development of a Phase 1 prototype set of hardware that has been submitted to the NSA for evaluation. The components utilized for this first development phase were the FC-X Inline Network Encryptor, the ES520 Deployable Mesh Point and the ES210 Tactical Mesh Point. The ES210 serves as a prototype wireless sensor interface module allowing the connection of serial and Ethernet sensors. The ES520 is the wireless access point and the FC-X serves as a Gateway for the network, providing an additional layer of security.

For the air monitoring system, the RS232 interface on the single board computer is connected to the ES210 wireless sensor interface module. The radiation level and system status data is then transmitted wirelessly from the ES210 to the process monitoring LAN where a computer displays and logs the data.

The wireless air monitoring system hardware has been installed in a field process environment for evaluation and testing. The screen wire ion chamber and wireless sensor network has been in operation for several months collecting data and undergoing routine

source checks. In order to further evaluate the effect of dust and dirt on the chamber, it is being operated without the 5 micron filter paper for part of the field evaluation and then with the paper for the remainder of testing. The data collection software receives the ion chamber data and logs important parameters including any errors or alarms for later examination.

In addition to the field testing, a lab mockup has been operating continuously with simulated sensor data and network performance monitoring. This testing has been valuable in refining the system's settings and operation during the development process. All network components are "pinged" for availability once per second and the information is archived for review. The lab results have shown that the wireless network can be highly reliable. So far the testing has been limited to a static non-mobile sensor arrangement with one sensor and one access point. Additional testing is planned with mobile sensor applications and roaming between access points.

Fortress has also recently delivered a prototype Suite B wireless network interface for thin client laptops and tablet computers. This interface will allow the connection of mobile operator and engineering computer assets to the secure network allowing more flexibility in the performance of daily operator rounds, process engineering walk downs and troubleshooting.

Conclusion

SRNL has developed a stand-alone radiation monitoring system utilizing a Suite B based ultra secure short range wireless sensor network. While the radiation sensor is specific to nuclear facilities, the short range wireless sensor network is applicable applications requiring high reliability with ultra secure protection of the wireless data network.

References

1. Wireless For a Nuclear Facility, Presented at the 53rd International Instrumentation Symposium May 8th, 2008.

2. Patent Application Industrial Universal Electrometer, Patent Application 12/311718 filed 10/10/2007.

3. Attix, Frank H., William C. Roesch and Eugene Tochilin, ed., Radiation Dosimetry, Vol. II, Instrumentation, 2nd Edition, New York, Academic Press, 1966.

4. NSA Suite B Cryptography, http://www.nsa.gov/ia/programs/suiteb_cryptography/

5. National Security Telecommunications and Information Systems Security Policy No. 11, Revised Fact Sheet National Information Assurance Acquisition Policy, July 2003.