Go Nuclear: Breaking Radiation Monitoring Devices

Ruben Santamarta
Principal Security Consultant, IOActive

Abstract

Radioactivity is a part of our environment; we are continuously exposed to natural radiation arising from the Earth and even from outer space. We are also exposed to artificial sources of radiation, derived from human activities. Ionizing isotopes are used across multiple sectors: agriculture, medicine, research, biochemistry, and manufacturing.

The need for sophisticated devices to measure and detect the presence of radiation seems clear. Critical infrastructure, such as nuclear power plants, seaports, borders, and even hospitals, are equipped with radiation-monitoring devices. This equipment detects and prevents threats ranging from smuggling nuclear material to radiation contamination.

The purpose of this research is to provide a comprehensive description of the technical details and approach IOActive used to discover vulnerabilities affecting widely deployed radiation monitoring devices. Our work involved software and firmware reverse engineering, RF analysis, and hardware hacking.

IOActive®

Contents

Introduction

"The use of nuclear energy must be safe; it shall not cause injury to people, or damage to the environment or property" (Nuclear Energy Act, 1954).

Radioactivity is a part of our environment; we are continuously exposed to natural radiation arising from the Earth and even from outer space. However, when people hear the word “radiation” they tend not to think of naturally occurring radioactive materials (NORM), but rather of accidents at Nuclear Power Plants (NPPs) or obscure threats, such as so-called “dirty bombs.” Unfortunately, the risks associated with man-made radiation are more familiar than its benefits.

There are several different types of radiation, however, in this research, we will be referring to ionizing radiation only. This type of radiation is capable of knocking electrons out of their orbits, altering the balance between electrons and protons, and giving an atom a positive charge. This basically means that when this type of radiation passes through matter, it may become electrically charged: ionized. Also, when ionizing radiation reaches live tissues, it may cause a disruption of normal biological processes, which results in serious diseases, such as cancer, or even fatalities.

In addition to NORM, we are also exposed to artificial sources of radiation, derived from human activities. Ionizing isotopes are used across multiple sectors: agriculture, medicine, research, biochemistry, and manufacturing. This initially may sound surprising, as people outside of these specific professional areas tend not to associate them with radiation. In addition, some industrial processes, such as oil and gas drilling and metal mining, may bring natural radionuclides to the surface from underground formations.

The following are the most prominent uses of man-made sources of radiation:

Medical Applications

Radiation is used for multiple techniques, from well-known X-ray machines to the fabrication of radioisotopes for diagnostics, as well as gamma cameras.

Industrial Applications

There are a plethora of scenarios where radiation is used in industrial processes: sterilization, nuclear gauges, food production, and even smoke detectors.

Military Activities

Nuclear test detonations have been carried out at several locations across the globe. Radioactive debris resulting from these activities provoked a “worldwide fallout” of radioactive particles. Also, there are a number of countries that maintain nuclear weapons plants for uranium enrichment or processing.

Nuclear Fuel Cycle

Nuclear fission is one of the most well-known uses of radiation. As a result, numerous countries maintain NPPs, where the heat generated by uranium fuel through fission is leveraged to power a generator.

Supplying fuel to NPPs requires a series of complex processes carried out at different sites, primarily uranium enrichment and conversion facilities and fuel fabrication facilities.

The fuel cycle involves:

- Uranium recovery
- Conversion
- Enrichment
- Reconversion
- Fuel fabrication
- Use of the fuel
- Reprocessing
- Interim storage
- Reprocessing of high-level waste
- Disposal

As previously mentioned, it is not possible for a single facility to provide all the requirements needed to fully complete the fuel cycle. As a result, fuel and waste transportation also plays a key role.

We have seen how radiation is present in our everyday lives, although we do not usually notice it, which is a good thing overall. But if we think about it, that is also a challenge for those whose daily job is to guarantee that facilities, procedures and processes where radioactivity is involved are safe, e.g., nuclear operators who are trained to make sure no one is harmed during the normal working conditions of NPPs or law enforcement, which needs to prevent radioactive materials smuggling across borders.

Research

United States, 1979: The Three Mile Island Nuclear Generating Station suffered a core meltdown. Operators were unable to cope with the ambiguous signals the plant's HMI was sending, leading to one of the most serious nuclear accidents on US soil.

Spain, 2007: Bypassing security checks, someone stole approximately 70 fuel pellets of uranium oxide from a nuclear fuel facility. They were later found abandoned nearby. How this material ended up there is still a mystery.

Are these scenarios possible today? Critical infrastructure, such as NPPs, seaports, borders, and even hospitals, are equipped with radiation-monitoring devices. This equipment detects and prevents threats ranging from smuggling nuclear material to radiation contamination.

The purpose of this research is to provide a comprehensive description of the technical details and approach used to discover vulnerabilities affecting widely deployed Radiation Monitoring Devices (RMDs). Our work involved software and firmware reverse engineering, RF analysis, and hardware hacking.

Radiation Monitoring Devices

The need for sophisticated devices to measure and detect the presence of radiation seems clear. This is the purpose of RMDs, although there is not a single device that is appropriate for all the potential scenarios we have introduced.

As a result, multiple Radiation Monitoring Instruments (RMIs) are adapted to each scenario where radioactivity level readings need to be taken. When characterizing RMDs, there are common features that most share, as well as certain functionalities that make them unique.

We can establish the following groupings according to the type of radiation these devices can detect and how they take measurements:

- Type of radiation: alpha, beta, gamma, neutron
- Ranges of energy: kV, MV
- Units: Counts (CPM), Roentgens (i.e. mR/hr), Accumulated Dose, Current Dose (gray or rad)

Depending on the technology implemented in the detector, we have:

- Ionization chambers
- Proportional counters
- Neutron
- Geiger-Müller counters
- Scintillator detectors

- Semiconductor detectors

Finally, taking into account their designated mission, we may identify the following items:

- Alarming Dosimeter
- Personal Radiation Detector
- Area Monitor
- Radioisotope Identification Device
- Backpack
- Mobile System
- Aerial System
- Portal Monitor
- Sensor Networks

This research is mainly focused on area monitors. Portal monitors were also evaluated, although the initial analysis revealed a complete lack of security in these devices, so further testing wasn't necessary to identify significant vulnerabilities.

Portal Monitors

Radiation Portal Monitors (RPMs) are a fundamental component of the policy that was implemented worldwide, especially after 9/11 in the US, to prevent the illicit trafficking of nuclear and radiological materials. According to the IAEA, the definition of illicit trafficking is *'the receipt, possession, use, transfer or disposal of radioactive material without authorization'*. Not all the potential issues this definition covers are related to criminal activities, there are radiological situations that can be prevented by the proper use of RPMs.

RPMs are usually found at checkpoints, such as those at sea or dry ports[1], road and rail border crossings, airports, or secure facilities. They automatically detect the presence of radioactive material carried by people or in vehicles passing through the detection area. While this is certainly effective, it is also prone to false (or innocent) alarms due to factors, such as a variation in the background levels, specific materials (e.g., heavy doors), or even nearby RF interferences. In order to avoid this situation, these devices usually perform continuous background monitoring, feeding a statistical model aimed to prevent false positives with these readings.

Before explaining the potential attacks against these systems, it is important to briefly introduce the common procedure that should be followed to properly operate a RPM:

[1] http://www.aapa-ports.org/files/SeminarPresentations/05_OpsIT_Simmons_Patrick.pdf

1. **Detection**

   A threshold is usually configured so that any radiation level exceeding this value will trigger an alarm.

2. **Verification**

   False alarms are often triggered, so operators need to double check that everything is correct. This can be done either by repeating the process with the same RPM or, usually, by using secondary, portable monitoring instruments.

3. **Assessments and Localization**

   Once an alarm has been verified, the scenario needs to be evaluated in order to decide on an appropriate response.

4. **Identification**

   It is important that these devices be capable of identifying the radionuclide, as it may trigger different kinds of responses. Identifying an isotope commonly found in nuclear smuggling should elicit a much different reaction than, for example, finding an isotope in recycled metal debris.

Vulnerabilities in Ludlum Portal Monitors

RPMs are interesting targets, but they are difficult to analyze without having a physical device. In order to get an initial insight into these devices, we analyzed publicly available binaries from the US company, Ludlum.

> *"Our product lines serve many different markets including nuclear power, national laboratories, homeland security, oil and gas exploration, mining, environmental, medicine, industry, government, solid waste and more[...] Ludlum has shipped over 2500 gateway systems to over 20 countries.[...] We have additionally received significant contracts by the US government and more recently by China for the more stringent homeland security applications along borders and ports"*[2]

RPMs for personnel and vehicles were reviewed, including the firmware for the following models:

Ludlum 53

"The Model 53 Gamma Personnel Portal detects gamma radiation in or on personnel passing through the portal from either direction."[3]

[2] www.ludlums.com

[3] http://safeguard.ludlums.com/component/virtuemart/market-1/nuclear-power-plants-104/personnel-gamma-portal-monitor-11-detail?keyword=53&Itemid=0

Figure1 - Ludlum 53 and Software (images from www.ludlums.com)

These devices implement a touchscreen to interact with the applications, which run a Microsoft Windows operating system. The main application running by default ("Supervisor.exe") implements two different privilege levels that allow technicians to perform calibration and maintenance tasks. Each of these levels is protected by a different password, which can be configured.

However, by reverse engineering the binary where this logic is implemented, a backdoor password was found. This backdoor grants the highest privilege ("Level 2") to the attacker. As a result, malicious personnel can bypass the RPM's authentication and take control of the device, which could be used to disable it, thus preventing the RPM from triggering proper alarms.

```
// Lmi.Sam.Supervisor.Host
private const string BackDoor = "5147";
```

```
// Lmi.Sam.Supervisor.Host
public void ValidatePassword(string Password)
{
    ApplicationSettings applicationSettings = Program.Monitor.Settings;
    this.currentPasswordLevel = Host.Level.None;
    if (Password == applicationSettings.PasswordDecrypt(applicationSettings.Level1Password))
    {
        this.currentPasswordLevel = Host.Level.Level1;
    }
    if (Password == applicationSettings.PasswordDecrypt(applicationSettings.Level2Password))
    {
        this.currentPasswordLevel = Host.Level.Level2;
    }
    if (Password == "5147")
    {
        this.currentPasswordLevel = Host.Level.Level2;
    }
}
```

Figure 2 - Backdoor Password

Gate Monitors - Model 4525

This device comes with monitoring software that it is installed on a companion Windows machine. This software allows collecting and archiving data from all available lanes, displays alarms, and generates reports. It can also capture images of vehicles passing through the detection area.

The communication between RPM units and software is performed through either LAN or wireless. There are two main protocols involved:

Figure 3 - 4525 Series (available at www.ludlums.com)

Discovery

Port 20034/UDP. This is the NetBurner discovery and configuration protocol. It lacks any security measure. Any attacker in the adjacent network can change the device's network settings, which opens the door to multiple attacks (e.g., man-in-the-middle).[4]

Ludlums

Port 23/TCP. This protocol is cleartext, so attackers would be able to falsify readings, disable alarms, or perform any other originally supported operation.

[4] http://ludlums.com/component/virtuemart/equipment-type-3/gate-monitoring-9/vehicle-gateway-monitors-295-detail?Itemid=2657

Attacks Against Ludlum Devices

Attacker Capabilities

Attackers need to gain privileged access in the wireless or LAN network to perform a man-in-the-middle attack. They can achieve this by either compromising other nodes in the network or breaking into the wireless network due to a poorly secured infrastructure.[5]

Stealth Man-in-the-Middle Attack

Malicious actors can perform a man-in-the-middle attack that alters the readings when the radioactive material they are interested in trafficking is detected. This would allow them to safely bypass these gate monitors while maintaining the compromised device in a working condition.

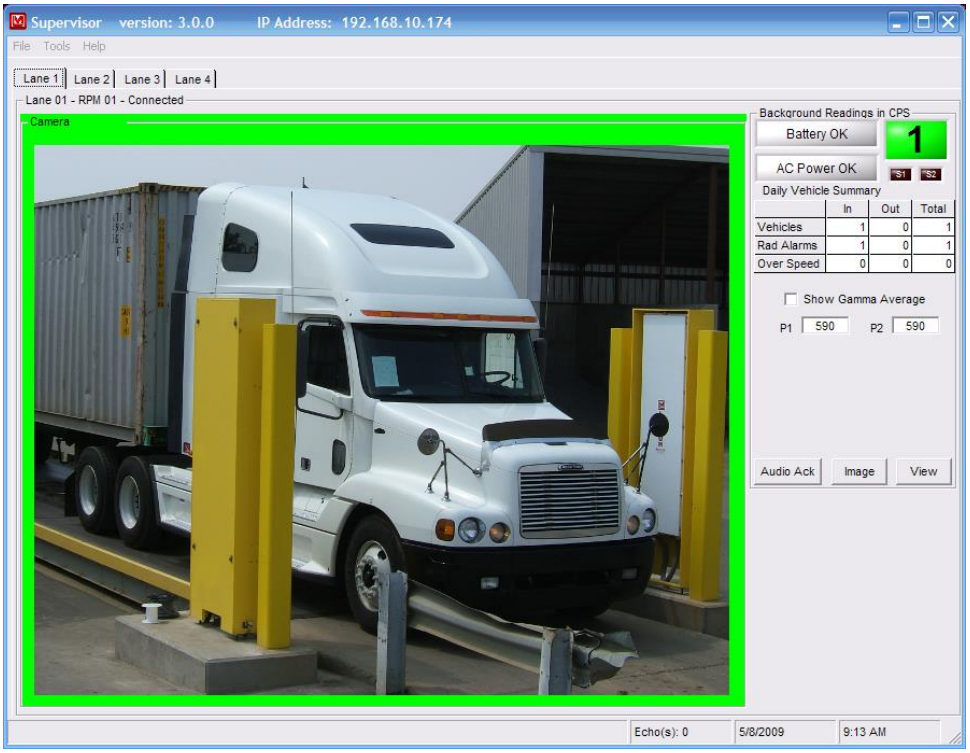


Figure 4 - Supervisor Application (available at www.ludlums.com)

Adequately resourced attackers can replicate a Ludlum gate monitor installation and tune malware based on empirical testing. IOActive used CERN's GEANT4[6] software, a toolkit

[5] http://ludlums.com/images/stories/product_manuals/Wireless_Connection_Installation.pdf)

[6] http://geant4.web.cern.ch/geant4/

for the simulation of the passage of particles through matter, to implement an initial simulation of a Plastic EJ-200 Scintillator, the same used in Ludlum's devices. Empirical measurements can be made up with information collected from EJ-200 datasheets[7] and publicly available information. Although the accuracy of this simulation will differ from a real environment, this was intended to demonstrate the possibility of deploying an advanced payload that hides specific isotopes from detectors, while providing the expected readings for others.

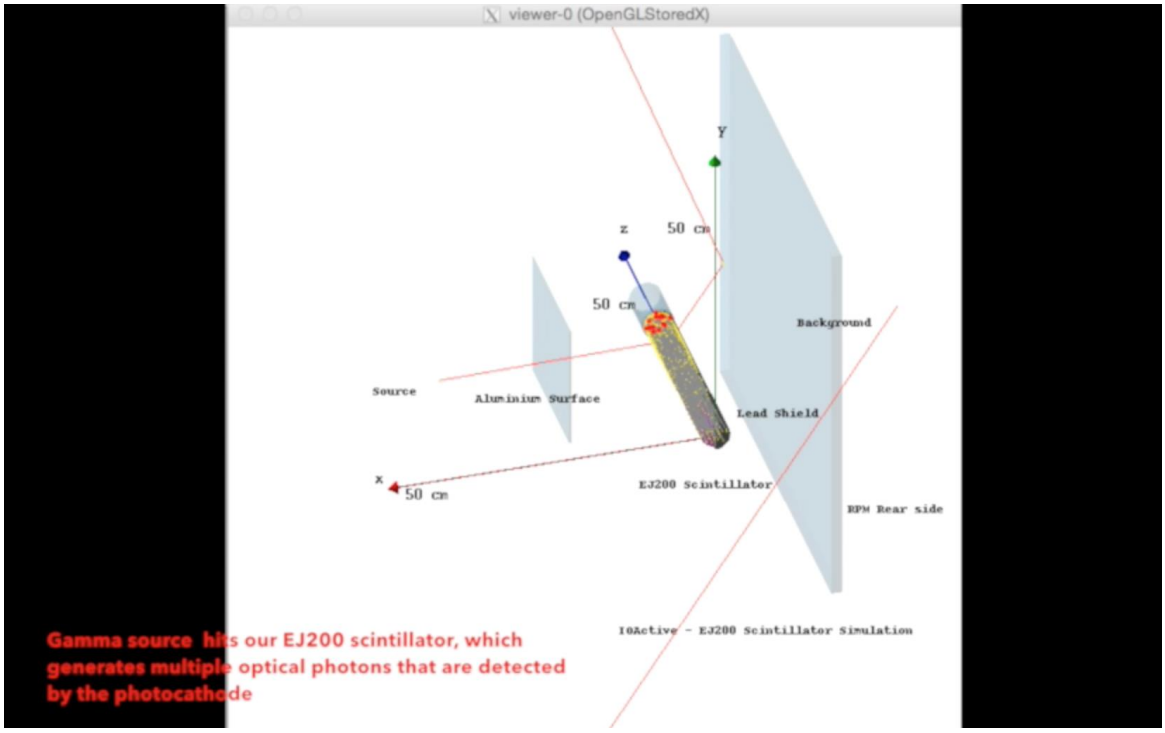


Figure 5 - EJ200 Simulation (Full Video Available on IOActive's YouTube Channel)

[7] http://www.ggg-tech.co.jp/maker/eljen/ej-200.html

Radiation Monitoring Systems for Nuclear Power Plants

NPPs apply the ALARA (as low as reasonably practicable) principle when assessing radiological risks. In general, NPPs are designed to ensure a high level of safety in their handling of nuclear materials and radiation sources.

Radiation monitoring systems aid plant personnel in:

- Protecting the health and safety of the public and plant personnel
- Assessing plant radiological conditions to identify and mitigate the consequences of abnormal plant events

Radiation monitoring systems also provide input to other plant systems, such as containment vent isolation or control room habitability.

Nuclear facilities should provide external and internal monitoring of individual occupational workers, including monitoring for external radiation, airborne contamination, and surface contamination. Also, they need to be properly equipped to protect the public: monitoring systems for effluents and environmental monitoring no matter the operational states (i.e., in normal operations or under accident conditions).

In order to comply with these requirements, an NPP would need to be fitted with, at least, two types of radiation monitoring instruments:

Stationary RMIs

Used to observe the radioactivity of liquids, rooms, facility processes, releases, spent nuclear fuel, nuclear waste, and the environment, as well as to provide information about fuel failures and radioactive substance leaks.

Portable, semi-portable, and locally installed monitoring equipment

A sufficient number of portable instruments need to be available at the NPP to complement stationary instruments. These devices are capable of measuring alpha, beta, gamma, and neutron radiation levels, and can be used in any operational conditions. For example, in case of an accident, portable equipment supporting teledosimetry and remote operation can provide valuable help when detecting contamination in hostile environments, while minimizing the exposure of personnel. Also, when stationary instruments are believed to be failing or not providing representative results, health physics and emergency response teams can use portable equipment to address the situation.

According to purpose, we can divide RMIs into the following categories:

Personnel Monitoring

Among the instruments designed to measure the internal and external dose individual workers may receive, such as dosimeters, NPPs also deploy portal monitors, as those introduced in the previous section.

Area Monitoring

This equipment needs to be deployed at specific locations, according to the facility's design. In general, we will find monitors to measure external dose rates, air and surface contaminations. Area radiation monitoring systems are strategically located within NPP and alert personnel when radiation levels are above limits prescribed by regulatory, health physics, and administrative controls. NPP area monitors include both stationary and portable monitors.

Process Monitoring

Gaseous and liquid systems are monitored to detect either system malfunctions or equipment failures that may result in radioactive leaks. RMDs for process monitoring will be present in ventilation exhaust ducts of reactor building, decontamination centers, process water discharge lines, moderator system heat exchangers, and steam lines, just to mention a few examples.

Waste Monitoring

Airborne effluents, such as Tritium, Argon-41, and particulate radioactive materials should be detected by these RMDs. The equipment is usually installed in the plant outfall line, as well as in those places designed to handle solid waste.

Environmental Monitoring

These RMDs need to be properly running under all operational states of the plant, in order to detect any increase in the background radiation levels within the facility's boundaries, as well as the designated areas around the NPP.

To summarize, the following 10 types of radiation monitoring equipment are found at a NPP:

1. Area radiation monitors (low range and high range) and accident monitors
2. Airborne contamination monitors
3. Surface contamination monitors
4. Personal contamination monitors for interzonal checkpoints
5. Portal monitors
6. Process radiation monitors
7. Effluent radioactivity monitors for liquid and gaseous effluents
8. Personal dosimeters, such as thermoluminiscent (TLDs), neutron, direct reading, or alarming
9. Portable radiation monitors and contamination monitors
10. Laboratory instruments

We still need to add another classification for these instruments. In an NPP, all the assets, such as Instrumentation and Control (I&C) instruments, hardware, or firmware,

need to be classified according to the impact of a failure in their normal working conditions. Based on this, we can separate instruments into two different categories:

1. Not important to safety: not in scope for this research
2. Important to safety: this includes safety and safety-related systems

Safety Systems

Systems provided to ensure the safe shutdown of the reactor or residual heat removal, or to limit the consequences of anticipated operational occurrences and design basis accidents. Examples of safety systems include: protection systems, safety actuation systems and safety system support features, such as power supply and HVAC. These are known as 'Class 1E' devices.

Safety-related Systems

Systems important to safety that are not safety systems. Examples of safety-related I&C systems include: the reactor control and limitation system, human-machine interface (HMI) panels, and our targets: radiation monitoring systems. It is important to note that whenever the Radiation Monitoring Device (RMD) triggers automatic actions, thus providing an input to the safety system, it would be safety classified.

Safety radiation monitoring systems are permanently installed and fitted with centralized remote displays and alarms in the control room. Other safety-related radiation monitoring instruments are also equipped with local alarms and their collected readings are transmitted to the control room, or a separate operational control center.

At this point, we understand what RMDs are used for and the underlying need for deploying them, but we still need to know where to do so. This is a key factor to guaranteeing successful monitoring.

Although the distribution of RMIs varies according to the NPP's design (e.g., depending on the reactor type), we can still identify multiple assets that need to be covered by RMDs. Before going further, we need to briefly introduce two key concepts in NPP design: Area Segregation and Zoning System.

Area Segregation

An NPP cannot be conceived as a flat facility; instead, it is segregated in different areas, mainly designated due to the anticipated risk of contamination:

- Controlled area: Access to this area needs to be controlled, providing protection measures to prevent the spread of contamination during normal working conditions or limit the extent of an exposure in case it occurs. Normally these areas are physically segregated and implement access control mechanisms.
- Supervised area: Not a controlled area, but exposure conditions are kept under review. Personnel entering a controlled area are at higher risk than in a supervised one, thus requiring tighter controls. This area does not need to be physically segregated, but only clearly demarcated. Also, access controls are

less restrictive than in controlled areas, so non-radiation workers may be permitted. This is important in terms of security.

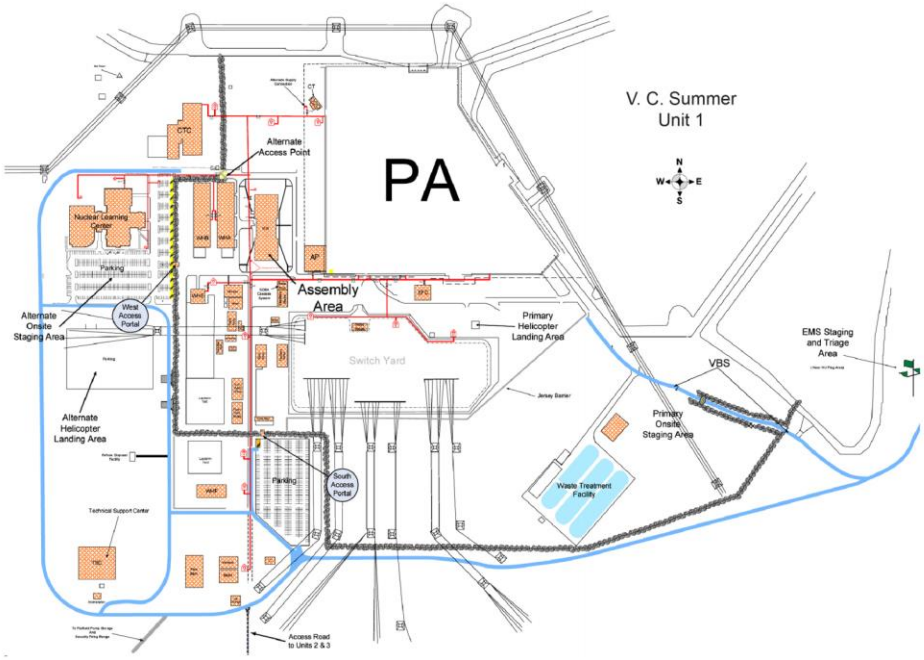


Figure A1-1 Unit 1 Facility Layout

Figure 6 - V.C. Summer NPP (US) Unit 1[8]

Zoning System

In order to minimize contamination and control its spread, the NPP should be divided into zones. Personnel moving from a low-risk zone to a higher risk one, and vice-versa for exit, need to pass through interzonal checkpoints, provisioned with portal monitors. As mentioned before, the ability to bypass any of these checkpoints by exploiting a vulnerability may cause a security breach.

In case of an accident, the NPP defines a series emergency response zones that cover multiple areas with a different radius of action, ranging from the contiguous area around the NPP to dozens of kilometers away for secondary zones.

[8] https://www.nrc.gov/docs/ML1104/ML110410260.pdf

Vulnerabilities in Mirion WRM2 Protocol

Affected Vendors

Mirion

"Our organization is comprised of over 1000 talented professionals, passionate about delivering world class products, services, and solutions in the world of radiation detection and protection. [...] In partnership with our customers in NPPs, military and civil defense agencies, hospitals, universities, national labs, and other specialized industries, Mirion Technologies strives to deliver cutting edge products and services that constantly evolve based on the changing needs of our customers"[9]

"The WRM2 System provides a means to monitor and supervise a population of various radiation monitors spread out over a large area. It wirelessly links devices equipped with WRM2 transmitters and can display their statuses and measurements on a computer comfortably outside the area where the radiation measurement is taking place"[10]

Digi[11]

"The Digi XBee-PRO XSC 900 MHz RF module features two times the throughput and 20 times less current draw than the previous XSC module, making it ideal for long-range sensor applications. The RF module features an ADF7023 transceiver from Analog Devices, delivering best-in-class distances up to 28 miles Line-of-Sight (LOS), along with low power consumption, drawing less than 2.5 uA in power down."[12]

In-scope Devices

In addition to Mirion, other vendors also commercialize WRM2-compatible products, some of them seem to be just rebranded versions of Mirion's. The scope for this research included the following devices:

1. **Laurus DRM2**

http://www.laurussystems.com/products/products_pdf/DRM2.pdf

This Area Monitor seems to be a rebranded version of Mirion's DRM.

[9] http://www.mirion.com

[10] https://www.mirion.com/products/wrm2-wireless-remote-monitoring-system/

[11] http://www.digi.com

[12] https://www.digi.com/products/xbee-rf-solutions/embedded-rf-modules-modems/xbee-pro-xsc

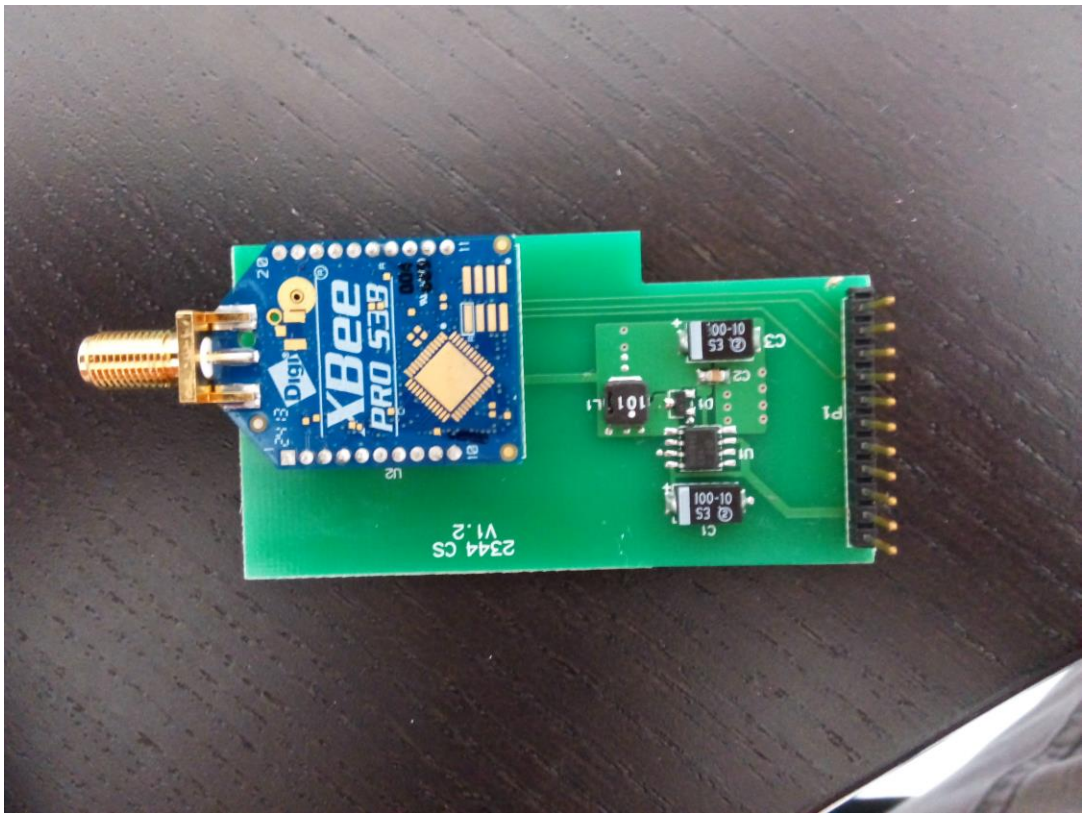


Figure 7 - WRM2 Radio Module - DRM2

https://www.mirion.com/products/drm-radiation-area-monitoring-system/

2. Mirion WRM-2

- Base Transceiver

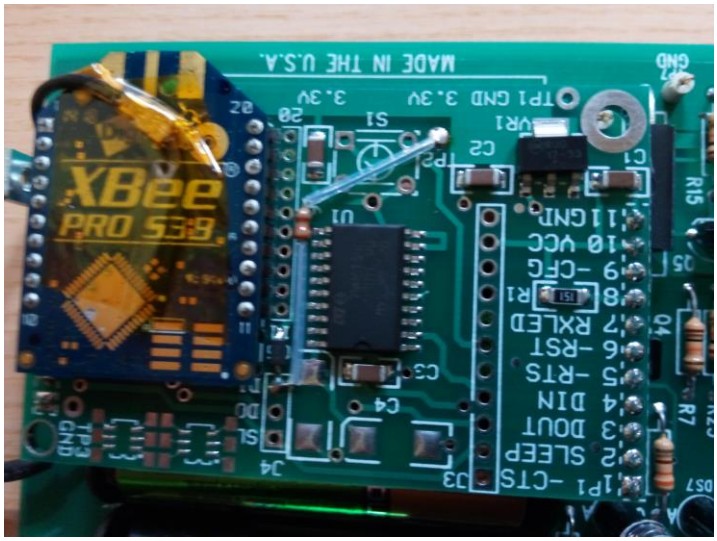


Figure 8 - Radio Module - WRM2 Base Transceiver

- IPAM-TX Teledosimetry module

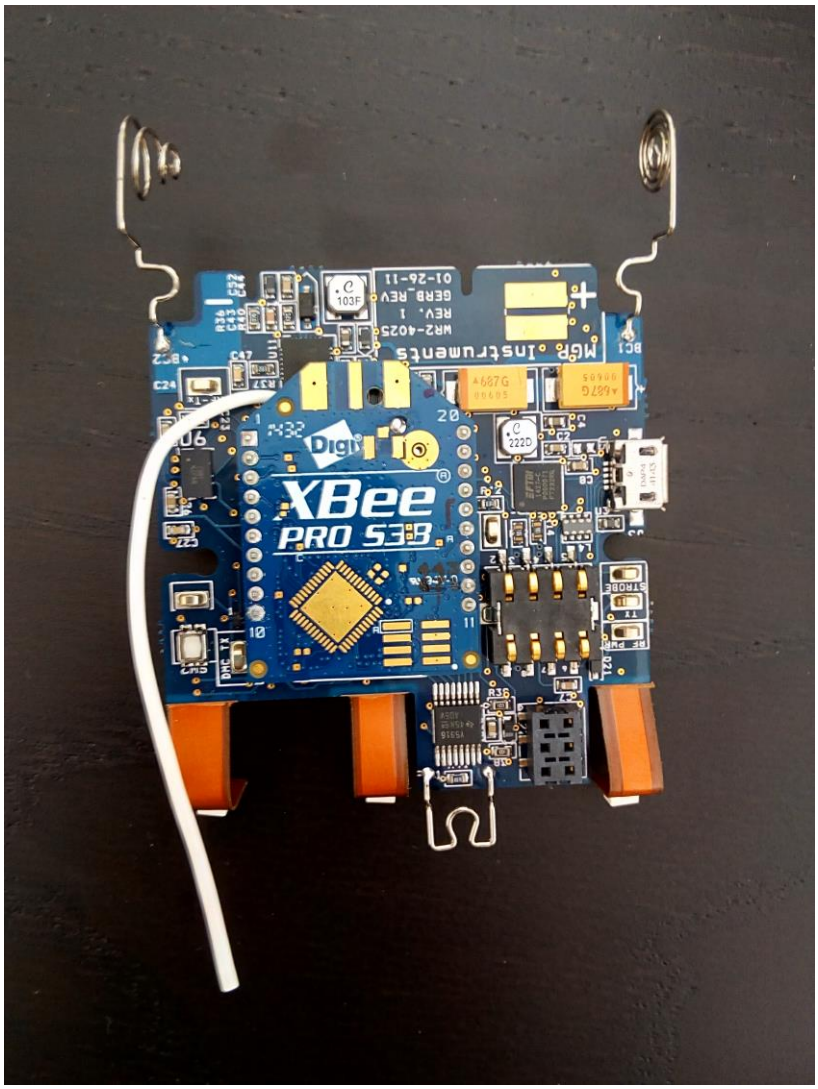


Figure 9 - Radio Module - IPAM Tx

https://www.mirion.com/products/wrm2-wireless-remote-monitoring-system/

Mirion's WRM2 standard is built on top of Digi's XBee S3B OEM modules, which implement a proprietary FHSS radio system. Mirion uses these radio modules to add on top its proprietary App Layer.

From Digi's official documentation:

> "*Networks are defined with a unique network identifier. For modules to communicate they must be configured with the same network identifier. The ID parameter allows multiple networks to co-exist on the same physical channel."*
>
> https://www.digi.com/resources/documentation/digidocs/pdfs/90002173.pdf

This Network ID is divided in two ranges:

- 0x10 - 0x7FFF Available
- 0x8000- 0xFFFE Read-Only (reserved for OEMs)

ID	0x27 (39d)	Module VID	User set table: 0x10 - 0x7FFF Read-only: 0x8000 – 0xFFFF	Networking	2	-

Figure 10 - Page 110 https://cdn.sparkfun.com/datasheets/Wireless/Zigbee/90002173_N.pdf

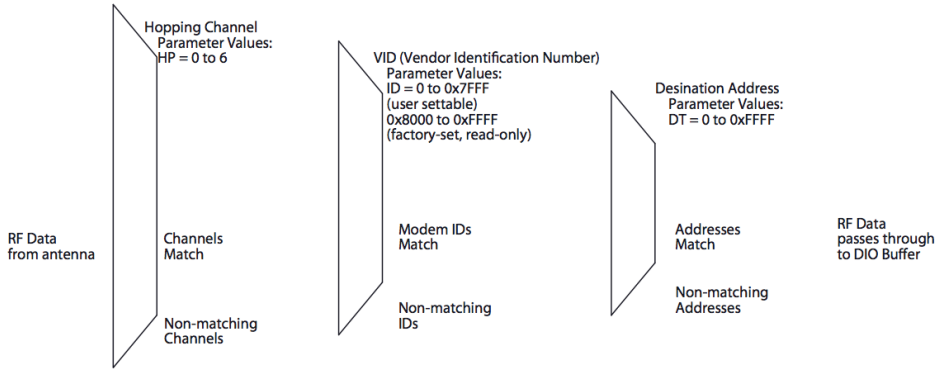
As a result, publicly available commercial modules cannot be configured to join a network in the OEM range module. Mirion's WRM2 uses the OEM Network ID 0x8160.

It is worth mentioning these Digi S3/S3B modules with XSC firmware are used not only for WRM2 products, but also across multiple sectors, including drones and telemetry for industrial systems. This means other OEM networks are also affected.

XBee-PRO XSC Addressing

Each RF packet contains addressing information that is used to filter incoming RF data. Receiving modules inspect the Hopping Channel (HP parameter), Vendor Identification Number (ID parameter) and Destination Address (DT parameter) contained in each RF packet. Data that does not pass through all three network security layers is discarded.

Filtration layers contained in the RF packet header



Header

The header contains network addressing information that filters incoming RF data. The receiving modem checks for a matching Hopping Channel (HP parameter), Vendor Identification Number (ID parameter) and Destination Address (DT parameter). Data that does not pass through all three network filter layers is discarded.

Figure 11 - Page 129 https://cdn.sparkfun.com/datasheets/Wireless/Zigbee/90002173_N.pdf

We analyzed these devices using three different approaches:

- Software and Firmware
- Radio
- Hardware

Software and Firmware

There are two different software applications involved:

- WinWRM2 (.NET)

  https://www.mirion.com/products/wireless-remote-monitoring-software/

  This software receives the inputs from the different radiation monitoring devices through the Base Station.

- XCTU (Java)

  https://www.digi.com/products/xbee-rf-solutions/xctu-software/xctu

  The Wireless functionality of the WRM2 systems is based on OEM XBee S3B 900Mhz transceivers.

  By reverse engineering the software it was possible to discover the encryption algorithm and keys used to encrypt the firmware that is used for the firmware files in the XSC-Pro and S3B-XSC compatible modules. This allows attackers to create a modified firmware.

XBee XSC Pro Firmware

Firmware files are encrypted using a hardcoded key discovered in the XCTU software. By reverse engineering the firmware it was possible to find:

- Seven FHSS patterns along with their corresponding frequencies
- XBee's AT command handlers to bypass the OEM Network ID read-only protection. Once this handler is patched, it effectively allows attackers to turn any commercial XBee S3/S3B module into a 'weaponized' one. Attackers can receive and transmit from/to any XBee XSC network.

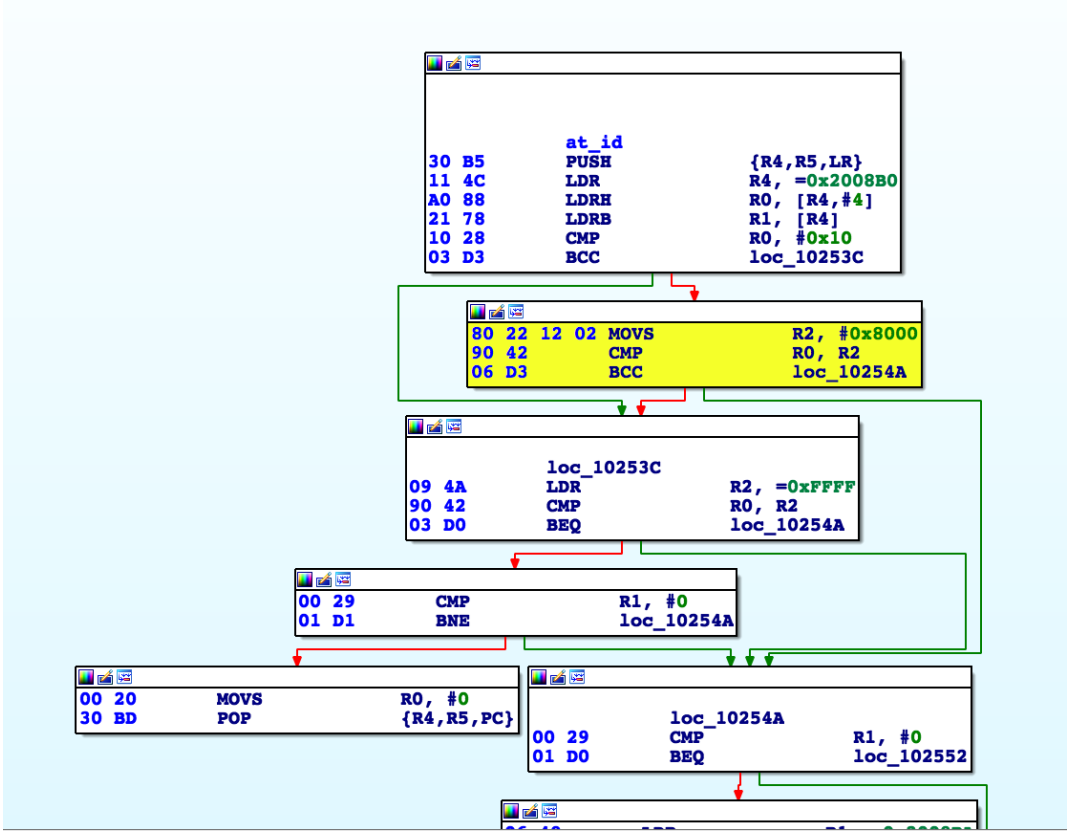


Figure 12 - AT ID Command Handler

Using this approach, an attacker can upload a new firmware to a regular XBee S3/S3B module to join any OEM network, including the network reserved for WRM2 standard (Network ID 0x8160).

Firmware Architecture: ARM (SoC: Silabs EFM32 GG)

Radio

For this approach, we analyzed the XBee XSC Pro proprietary FHSS-based radio system from scratch, using GNURadio and USRP B200 just to capture raw IQ data. It was possible to characterize the signal to understand how to:

- Identify the modulation used (GFSK)

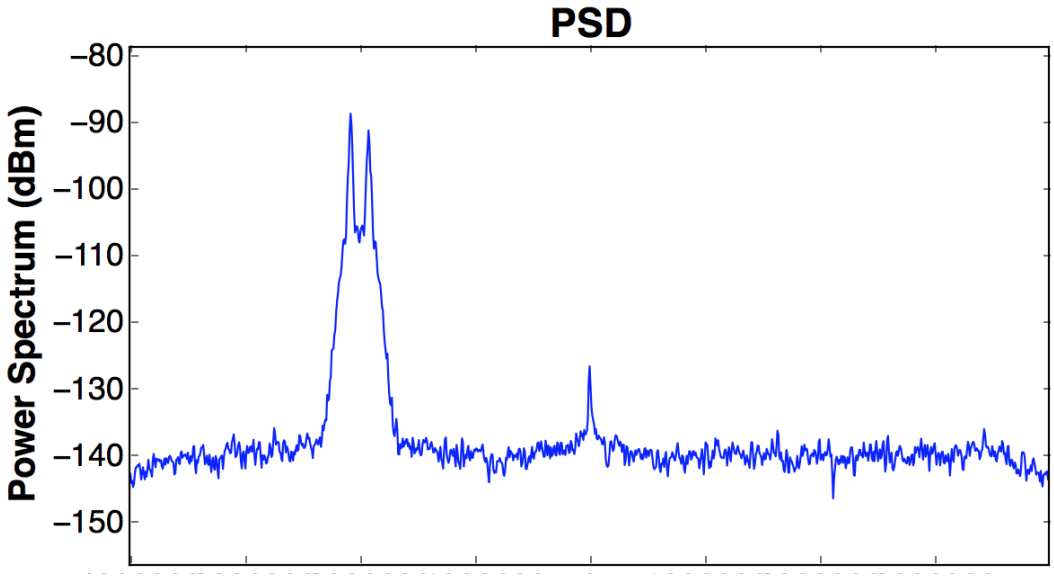


Figure 13 - GFSK Modulation

- Automatically Identify the channels, center Frequency and Hopping Patterns.
- Data encoding (Biphase-S)

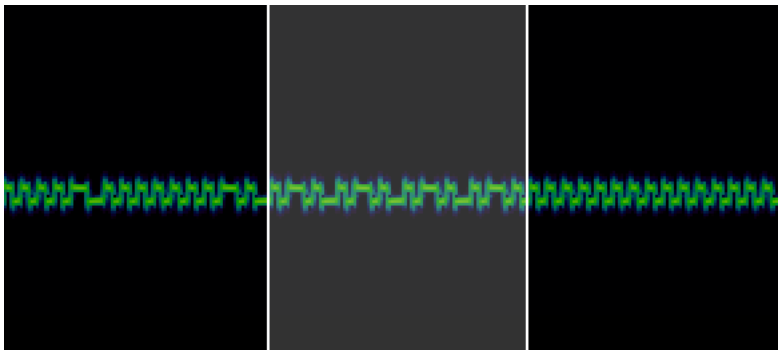


Figure 14 - RF capture showing Network ID (2 bytes - 0x5555)

Some of these steps were implemented using a custom C tool based on liquidSDR.[13]

[13] https://www.liquidsdr.org

Hardware

For this approach, we analyzed the XBee S3B front-end module by implementing a common hardware hacking methodology:

1. Mechanical tools, such as a Dremel, were used to remove the metallic cover.
2. Key components were identified and the intra-module connection map was built (ADF7023 transceiver, Silabs EFM32).

Figure 15 - Exposed Digi S3B Module

3. The SPI bus was tapped to capture, decode and interpret transmissions. As a result, the following data was collected:

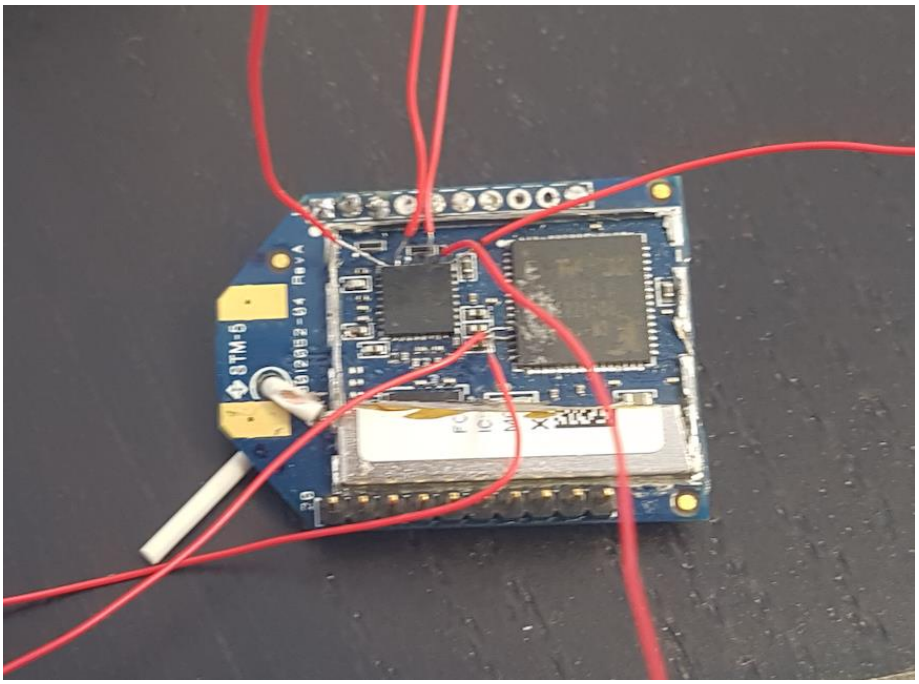


Figure 16 - Tapped SPI Bus

i. Custom firmware for an 8-bit RISC processor implemented inside the ADF7023 Transceiver.

ii. RF Calibration, channel and Hopping logic

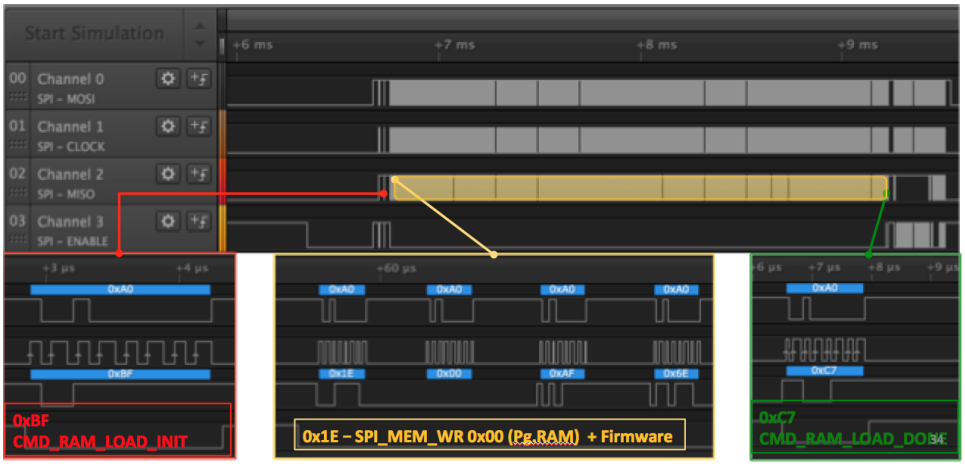


Figure 17 - Saleae Logic Analyzer

Attacks against Mirion WRM2-capable Radiation Monitoring Devices at Nuclear Power Plants

Attacker Capabilities

- Forging or sniffing WRM2 transmissions, either by repurposing a Digi S3/S3B XBee Module or by implementing the XSC and WRM2 protocol layers in a SDR device.
- Being located within the supported range for WRM2 transmissions. This may vary depending on the number of repeaters or the power used in the equipment to transmit the signals. In any case, they may be located dozens of miles away from the targeted NPP.

According to the operational state of the targeted NPP, there are two worst-case scenarios:

1. Normal working conditions
2. Accident conditions

NPP in Normal Working Conditions

The NPP is operating in the normal state, with all the systems properly functioning.

'Radioactive Leak' Attack

1. Using open-source intelligence (OSINT)[14] attackers collect either the Emergency Response Plan, or any other document that contains the Emergency Action Level[15] (EAL)[16] Response Matrix for the target NPP. Some of these documents can be found publicly available [17][18]
2. Attackers review the 'Abnormal Rad Release / Radiological Effluent' section to assess the initiating condition (IC)[19] that can be triggered using their current capabilities.

[14] https://www.mail-archive.com/powernet@hpspowernet.org/msg00186.html

[16] https://www.nrc.gov/docs/ML0804/ML080450149.pdf

[17] Virgil C. Summer Power Plant (US) https://www.nrc.gov/docs/ML1104/ML110410260.pdf

[18] Prairie Island (US) https://www.xcelenergy.com/staticfiles/xe/Regulatory/Regulatory%20PDFs/PI-EAL-RM.pdf

[19] One of a predetermined subset of nuclear power plant conditions where either the potential exists for a radiological emergency, or such an emergency has occurred.

3.1 **Emergency Action Level Matrix**

ABNORMAL RAD RELEASE/RAD EFFLUENT EALs

Table 3-R-1: Recognition Category "R" Initiating Condition Matrix

GENERAL EMERGENCY	SITE AREA EMERGENCY	ALERT	UNUSUAL EVENT
RG1.1 Valid reading on any monitors that exceeds or is expected to exceed Table R-1 column "GE" for ≥15 min. *Op. Modes: All*	**RS1.1** Valid reading on **any** radiation monitors that exceeds or is expected to exceed Table R-1 column "SAE" for ≥15 min. *Op. Modes: All*	**RA1.1** Valid reading on **any** Gaseous monitors > Table R-1 column "Alert" for ≥15 min. (Note 2) *Op. Modes: All*	**RU1.1** Valid reading on **any** gaseous monitors > Table R-1 column "UE" for ≥60 min. (Note 2) *Op. Modes: All*
RG1.2 Dose assessment using actual meteorology indicates doses >1,000 mRem TEDE or 5,000 mRem thyroid CDE at or beyond the site boundary.	**RS1.2** Dose assessment using actual meteorology indicates doses >100 mRem TEDE or 500 mRem thyroid CDE at or beyond the site boundary. *Op. Modes: All*	**RA1.2** Valid reading on Liquid monitor RM-L9 > Table R-1 column "Alert" for ≥15 min. (Note 2) *Op. Modes: All*	**RU1.2** Valid reading on Liquid monitor RM-L9 > Table R-1 column "UE" for ≥60 min. (Note 2) *Op. Modes: All*

Figure 18 - EAL Matrix For V.C Summer NPP (US)[20]

3. Attackers perform a passive recognition of the WRM2 radio transmissions in the area close to the NPP. From this collected data, they select the set of RMD IDs that will be spoofed. These IDs are sent in the WRM2 frames, at the start of the packet, before the radiation measurements.

Figure 19 - DRM WRM2-Capable RMD - Auxiliary Building Roof - V.C. Summer NPP (US)[21]

[20] Virgil C. Summer Power Plant (US) Emergency Plan https://www.nrc.gov/docs/ML1104/ML110410260.pdf
[21] http://i-i-s.net/wspdfs/2012%20Benchmark/Mirion%20Perimeter%20Monitoring.pdf

4. Attackers prepare the dataset of falsified readings that they want to transmit to simulate a radiation leak. Before sending these measurements, attackers may decide to perform a Denial-of-Service (DoS) against the legitimate WRM2-capable devices, by interfering at the right moment with the frames being sent. Malicious actors can launch this attack as the Digi's XSC FHSS hopping pattern is known and timings can be calculated. Instead of using this previous DoS step, attackers may directly transmit their falsified readings, which will be collected by the base transceiver and transmitted to the software that processes this data.

Eventually, alarms and readings will be consumed by operators. For those WRM2 devices being attacked that are safety-related (meaning they do not trigger automatic actions), the final decision on how to handle this situation is made by the operators and authorities according to the NPP's EAL scheme[22] and design documents. For them to decide if they should initiate a reactor shutdown or take any other protective action, it has to be clear that there is a need for human intervention, unless there is a design choice that enables these WRM2-capable devices to trigger automatic actions.

NPP Under Accident Conditions

'Sabotaging Health Physics/Emergency Response Teams' Attack

In certain NPP designs, WRM2-capable devices are used under accident conditions, by Health Physics/Emergency Response Teams. This can lead to the following scenarios:

Failed Evacuation

Readings collected from WRM2-capable area monitors provide the Health Physics/Emergency Response Teams with information about the progression of the radioactive plume. In case of an evacuation of personnel or population within the NPP designated zones, attackers may falsify these readings to trick authorities into giving the wrong directions for the evacuation, thus increasing the damage and/or potential casualties.

[22] https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/emerg-action-level-dev.html

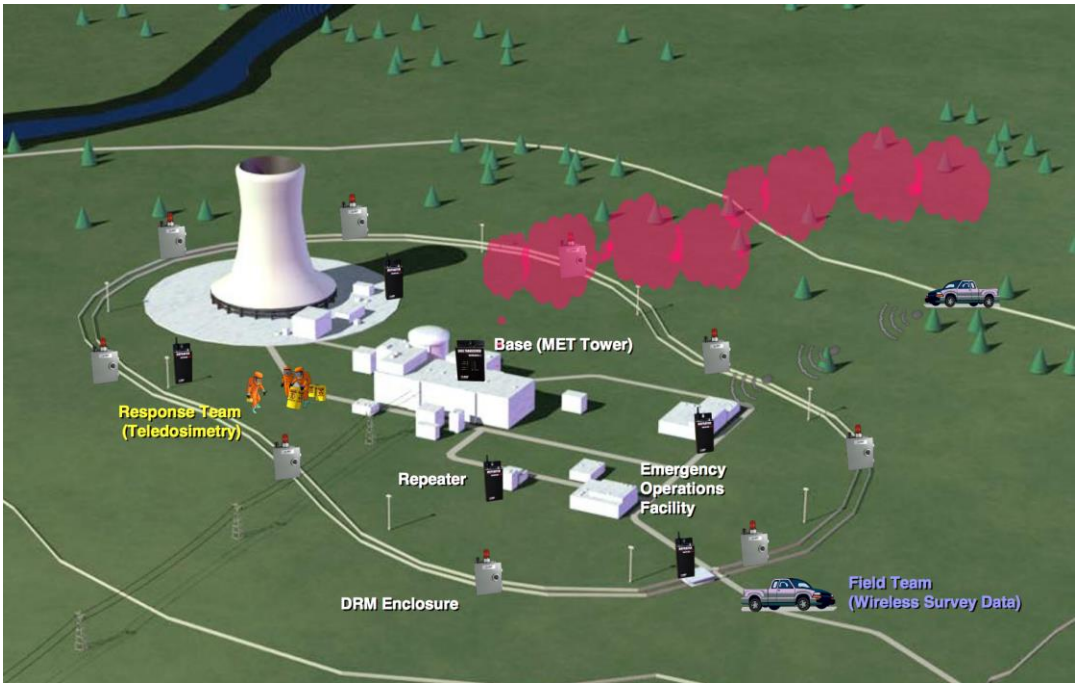


Figure 20 - WRM2 RMDs Use Under Accident Conditions[23]

Concealed Persistent Attack

Time is crucial when reacting to incidents involving radioactive materials. Attackers may look to increase the time an attack against a nuclear facility or an attack involving a radioactive material remains undetected, by sending normal readings to trick operators into thinking measurements are perfectly fine.

Mitigations in Real-world Scenarios

Certain mitigations are inherent to common NPP designs. Specific facilities within the plant are so protected that RF will be unable to penetrate them. For example, WRM2-capable devices located inside the reactor building will be almost impossible to be penetrated from outside via RF. This mitigation applies for Mirion WRM2 underwater equipment, which helps nuclear divers monitor the dose they are receiving while diving in the reactor pool. A similar scenario would happen in the control-room.

[23] http://i-i-s.net/wspdfs/2012%20Benchmark/Mirion%20Perimeter%20Monitoring.pdf

Responsible Disclosure

IOActive enforces a responsible disclosure policy. As a result, all affected vendors were contacted either directly or through the ICS-CERT [24](US) and CNPIC[25] in Spain. IOActive provided all technical details and maintained conversations with both Digi and Mirion to discuss the impact and feasibility of patching these issues.

This summarizes the vendors' initial responses:

1. Ludlum acknowledged the report, but refused to address the issues. According to them, these devices are located in secure facilities, which is enough to prevent exploitation.
2. Mirion acknowledged the vulnerabilities, but will not patch them as it would break WRM2 interoperability. Mirion contacted their customers to warn of this situation. They will work in the future to add additional security measures.
3. Digi acknowledged the report, but will not fix the issues as they do not consider them security issues.

Since the initial responses, IOActive was more recently contacted by Digi, indicating there is collaborative work between Digi and Mirion taking place to patch critical vulnerabilities uncovered in the research. In conclusion, we should acknowledge these issues are not currently patched, so increasing awareness of the possibility of such attacks will help to mitigate the risks.

[24] https://ics-cert.us-cert.gov/

[25] http://www.cnpic.es/

About Ruben Santamarta

Ruben Santamarta is experienced in network penetration and web application testing, reverse engineering, industrial control systems, transportation, RF, embedded systems, AMI, vulnerability research, exploit development, and malware analysis. As a principal consultant at IOActive, Mr. Santamarta performs penetration testing, identifies system vulnerabilities and researches cutting-edge technologies. Mr. Santamarta has performed security services and penetration tests for numerous global organizations and a wide range of financial, technical, and educational institutions. He has presented at international conferences including Ekoparty, 4SICS, and Black Hat USA.

About IOActive

IOActive is a comprehensive, high-end information security services firm with a long and established pedigree in delivering elite security services to its customers. Our world-renowned consulting and research teams deliver a portfolio of specialist security services ranging from penetration testing and application code assessment through to semiconductor reverse engineering. Global 500 companies across every industry continue to trust IOActive with their most critical and sensitive security issues. Founded in 1998, IOActive is headquartered in Seattle, USA, with global operations through the Americas, EMEA and Asia Pac regions. Visit www.ioactive.com for more information. Read the IOActive Labs Research Blog: http://blog.ioactive.com. Follow IOActive on Twitter: http://twitter.com/ioactive.

