JULY 22-27, 2017

MANDALAY BAY / LAS VEGAS

#BHUSA / @BLACKHATEVENTS

IOActive

Ruben Santamarta

- Principal Security Consultant, IOActive
  - Embedded
  - Reverse Engineering
  - RF
  - Hardware Hacking
  - Transportation

Agenda

1. Introduction
2. Portal Monitors – Ludlum
    1. Pedestrian
    2. Vehicle
3. Radiation Monitoring Systems - Mirion
    1. WRM2 Protocol
    2. Affected products
    3. Methodology and vulnerabilities
4. Attacks
5. Responsible disclosure

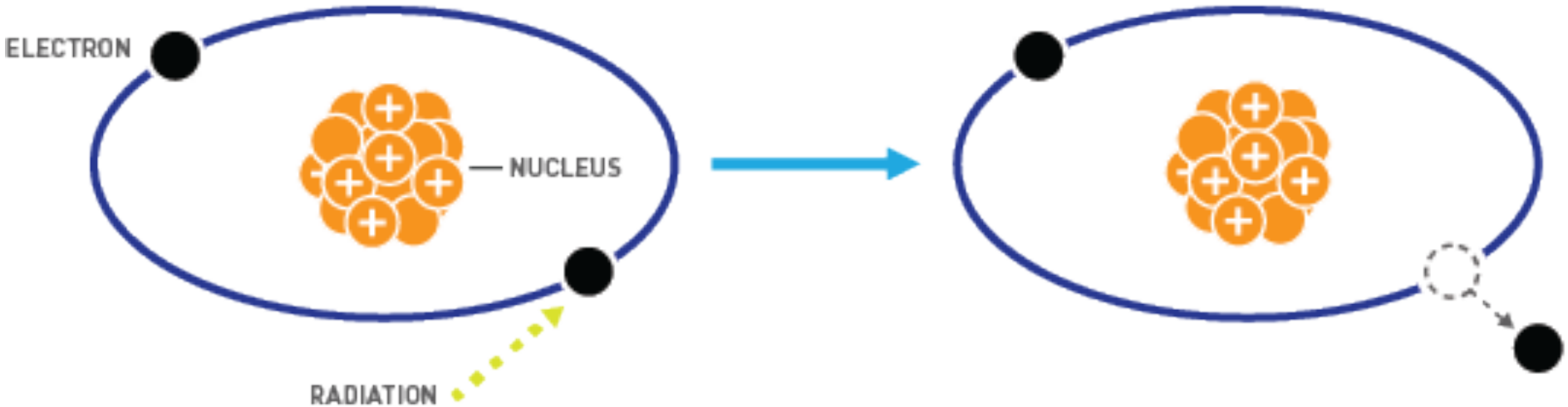
Three Mile Island, US

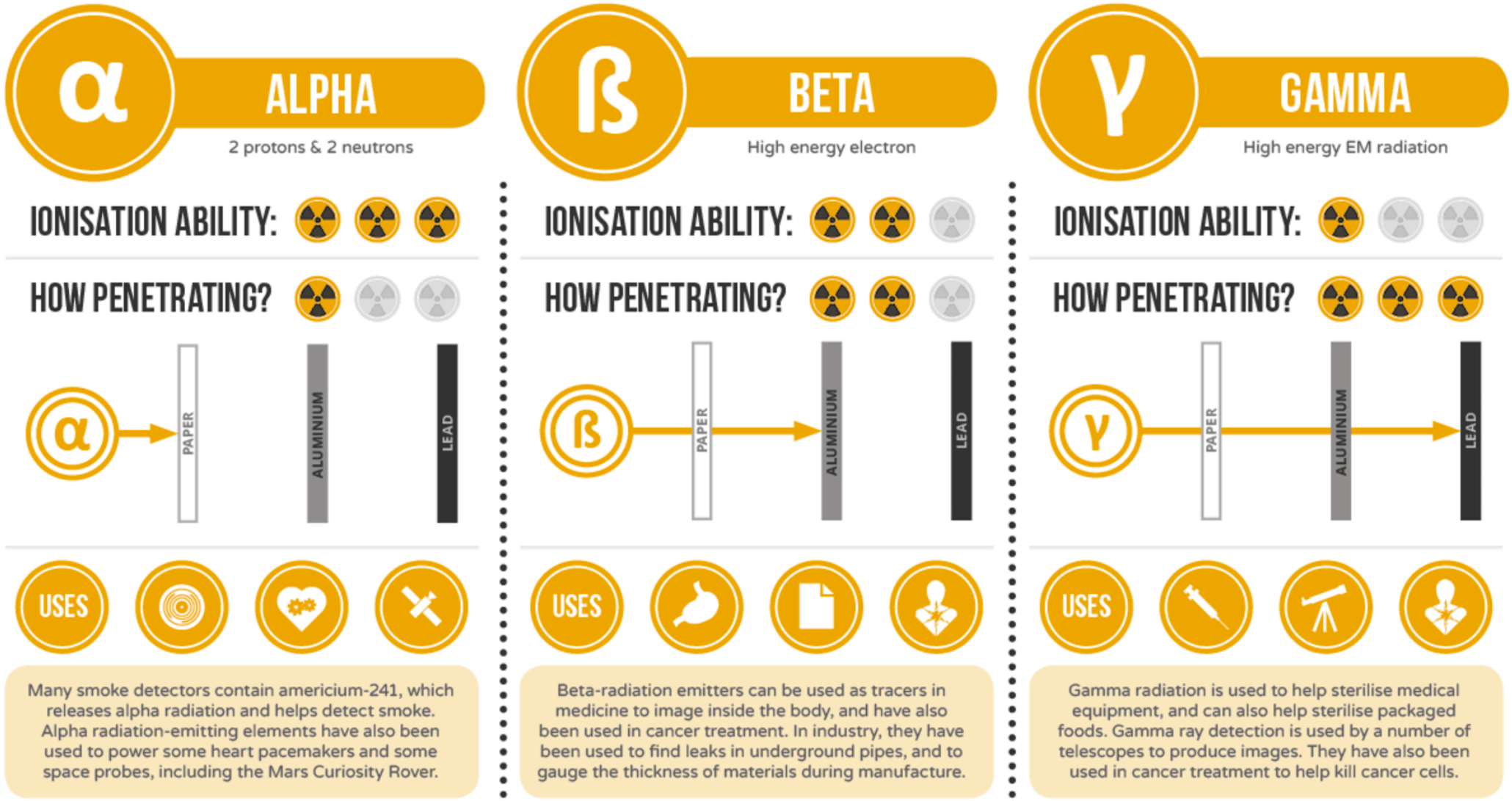
Juzbado, Spain

Juzbado, Spain (September 2007)	Guards at a fuel-element-producing facility found uranium tablets along a perimeter fence, in what authorities believe was an attempt by a member of the workforce to smuggle the goods out of the complex.[84]	Potential theft for illicit trade

https://www.stimson.org/sites/default/files/file-attachments/Nuclear-Energy-web-122315.pdf

IONIZING RADIATION





http://www.compoundchem.com/wp-content/uploads/2015/09/A-Guide-to-Different-Common-Types-of-Radiation.png

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****"*

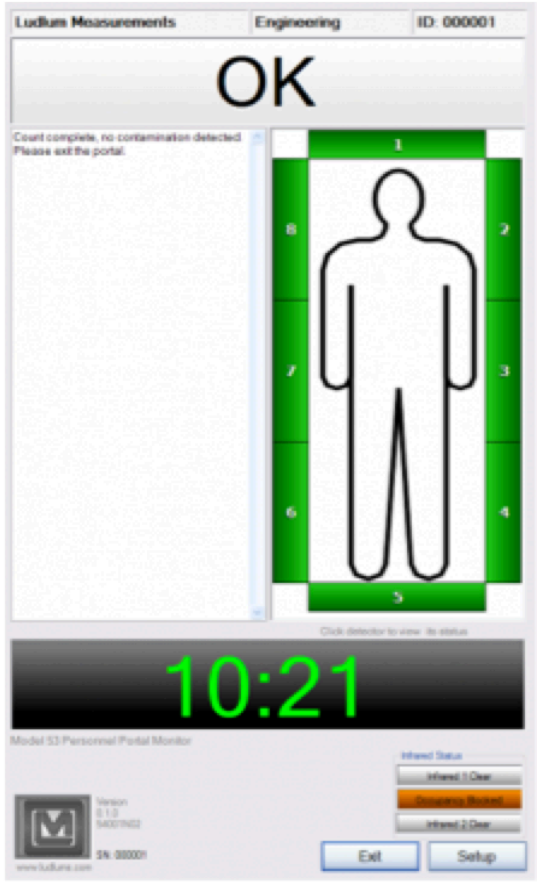
www.ludlums.com

PORTAL MONITORS

- Sea/Dry Ports
- Border Crossings
- Airports
- Nuclear Power Plants

Frank Franklin II/ASSOCIATED PRESS

Pedestrian




```
// 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;
    }
}
```

BackDoor = “5147”

Image by www.ludlums.com

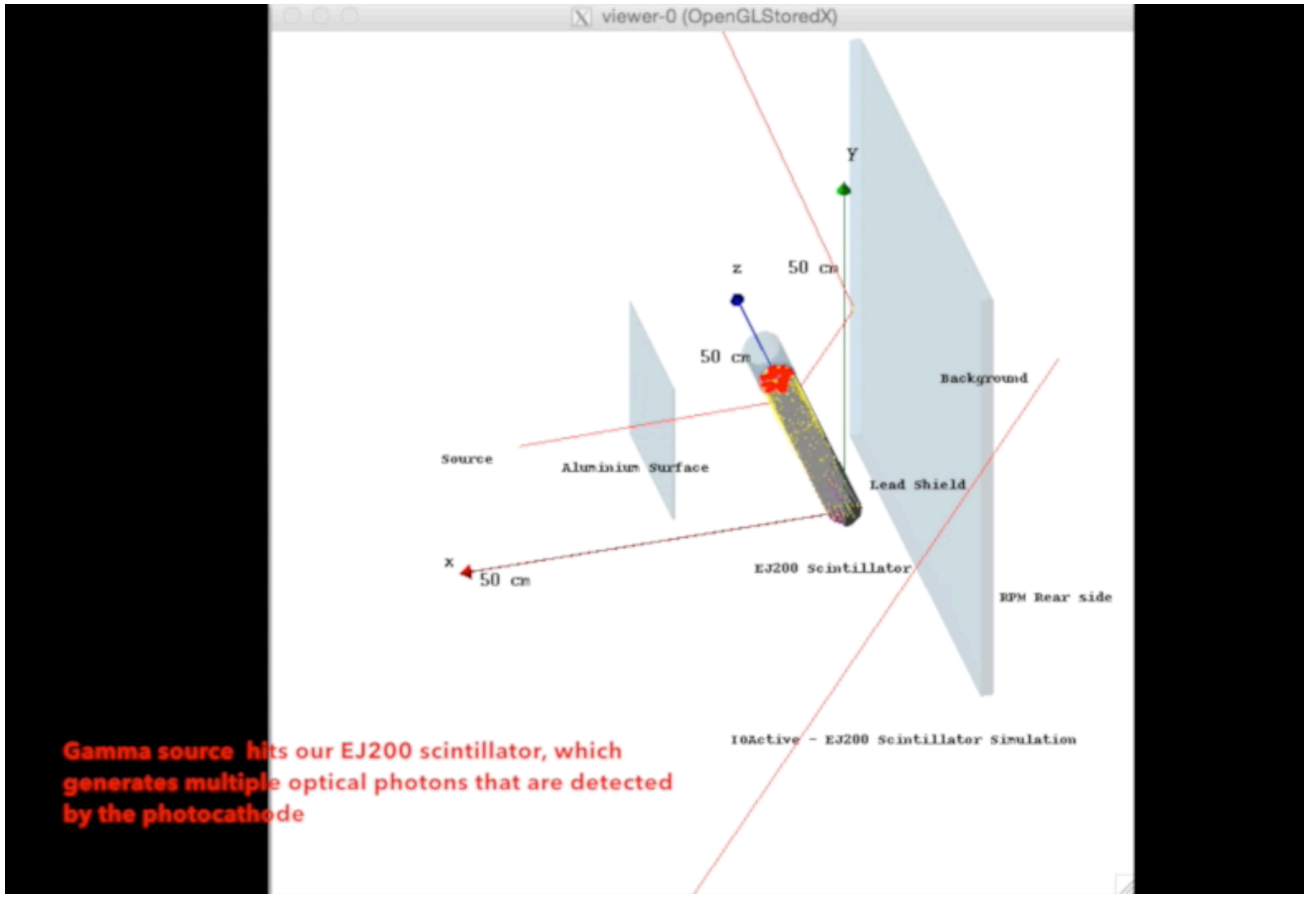
Vehicles

Image by www.ludlums.com

4525 SERIES

- 20034/UDP
  - NetBurner Discovery and Configuration
- 23/TCP
  - Ludlum Clear-Text Protocol

Stealth Man-in-the-middle Attack

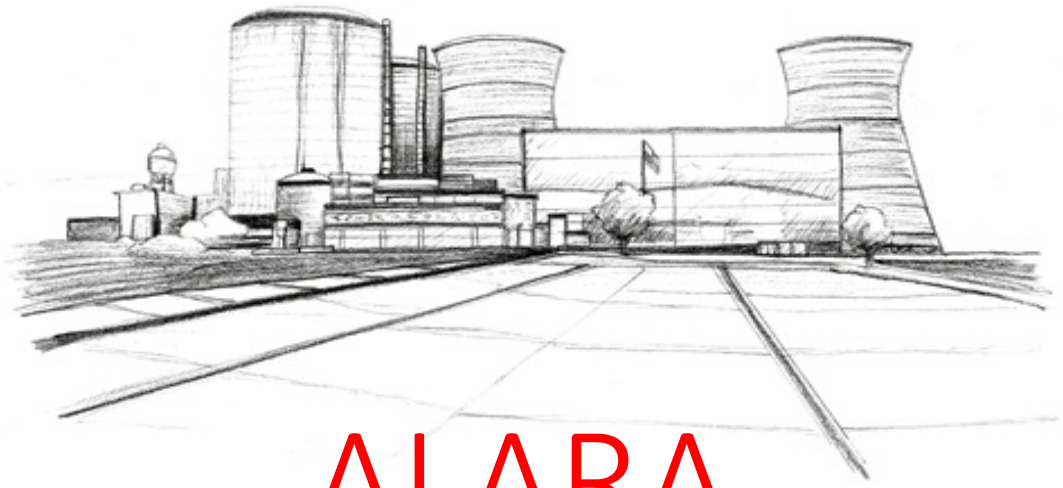


- Hides specific isotopes
- CERN's GEANT4
  http://geant4.web.cern.ch/geant4/
- EJ200 Scintillator

Full video Available on IOActive's Youtube Channel

Radiation Monitoring Systems

Image by Mike Walker



ALARA

As Low As Reasonably Achievable

RMDs 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
- Monitoring effluents and environmental monitoring no matter the operational states.

RMDs provide:

- ✖ Input to safety systems (Class 1E)
- ● Data to be consumed by operators

- Portable, semi-portable or locally installed equipment

1. Alpha, beta, gamma, neutron
2. Teledosimetry
3. Remote operation
4. Health Physics/ Emergency Response Teams

Purpose

- Personnel
- Area
- Process
- Waste
- Environmental

Safety

- Not important to safety
- Important to safety
  - Safety Systems
    - Protection systems, safety actuation systems,
    - Power Supply, HVAC
    - 1E
  - Safety-Related Systems
    - **Radiation Monitoring Systems**
    - HMIs

Area Segregation

- Controlled
- Supervised

Controlled >> Supervised

http://www.pilgrimpower.com/about-us/photo-gallery.html

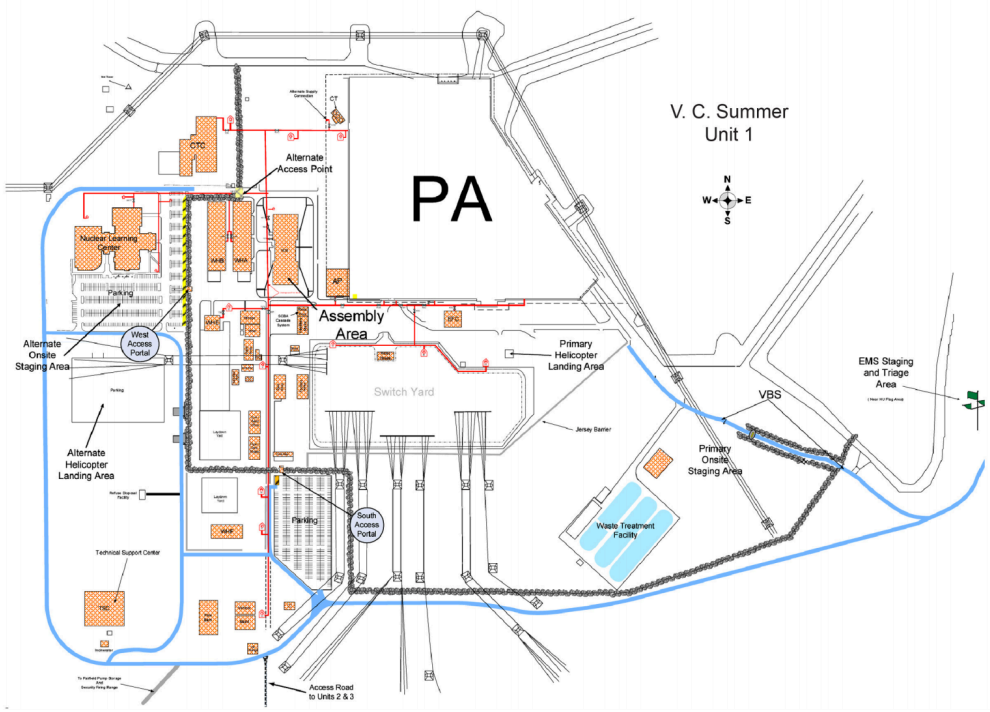
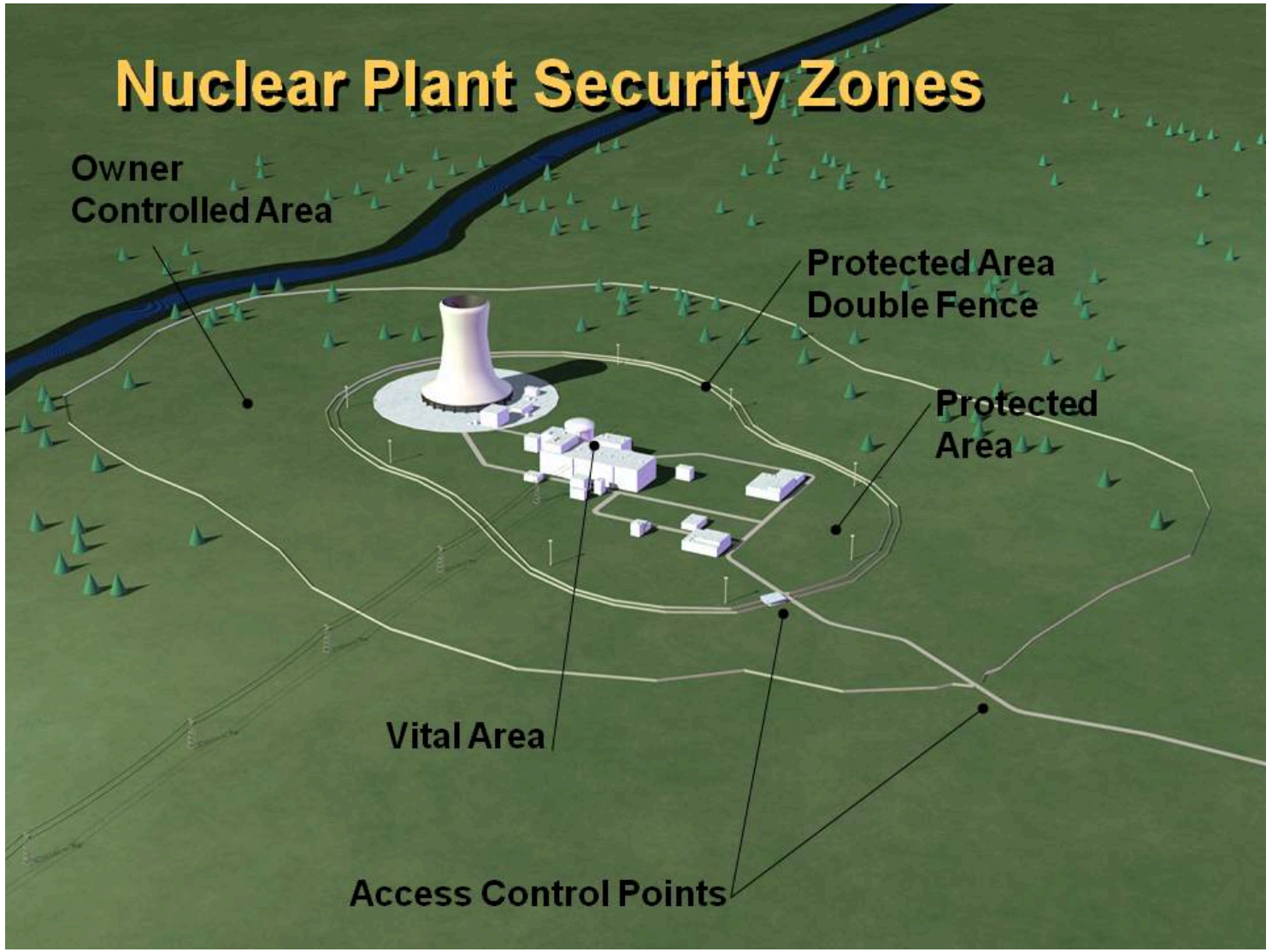


Figure A1-1 Unit 1 Facility Layout

V.C. Summer NPP (US) Unit 1

https://www.nrc.gov/docs/ML1104/ML110410260.pdf



https://public-blog.nrc-gateway.gov/2011/07/26/access-authorization-regulations-lead-to-arrest/

Mirion – WRM2

PRODUCT DESCRIPTION

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.

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

DRM-1 (GM)

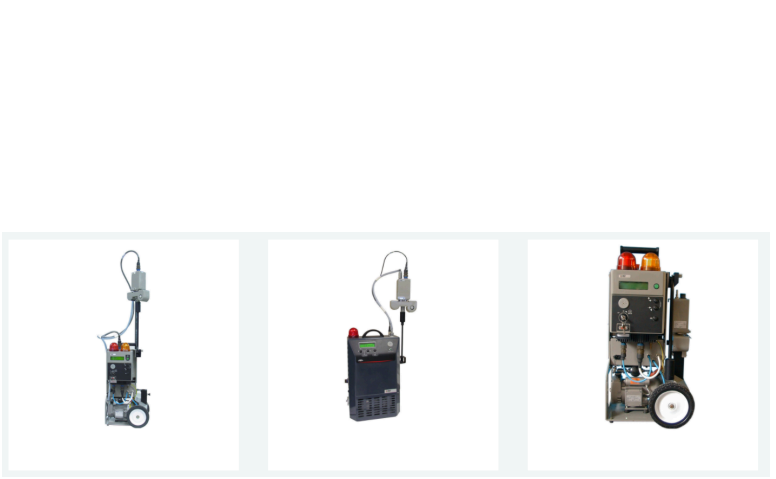
DRM-1D (CsI)

DRM-2(D)

Remote Display Unit

DRM-2(E)

Base Transceiver



ABPM 203/4M

https://www.mirion.com/products/particulate-monitors-2/

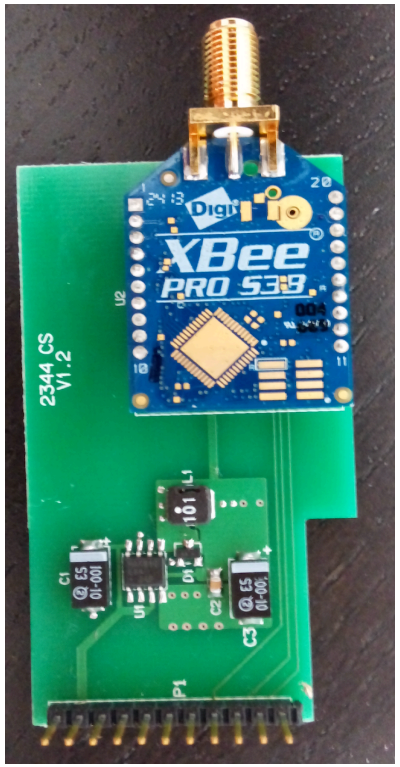
MESH Repeater

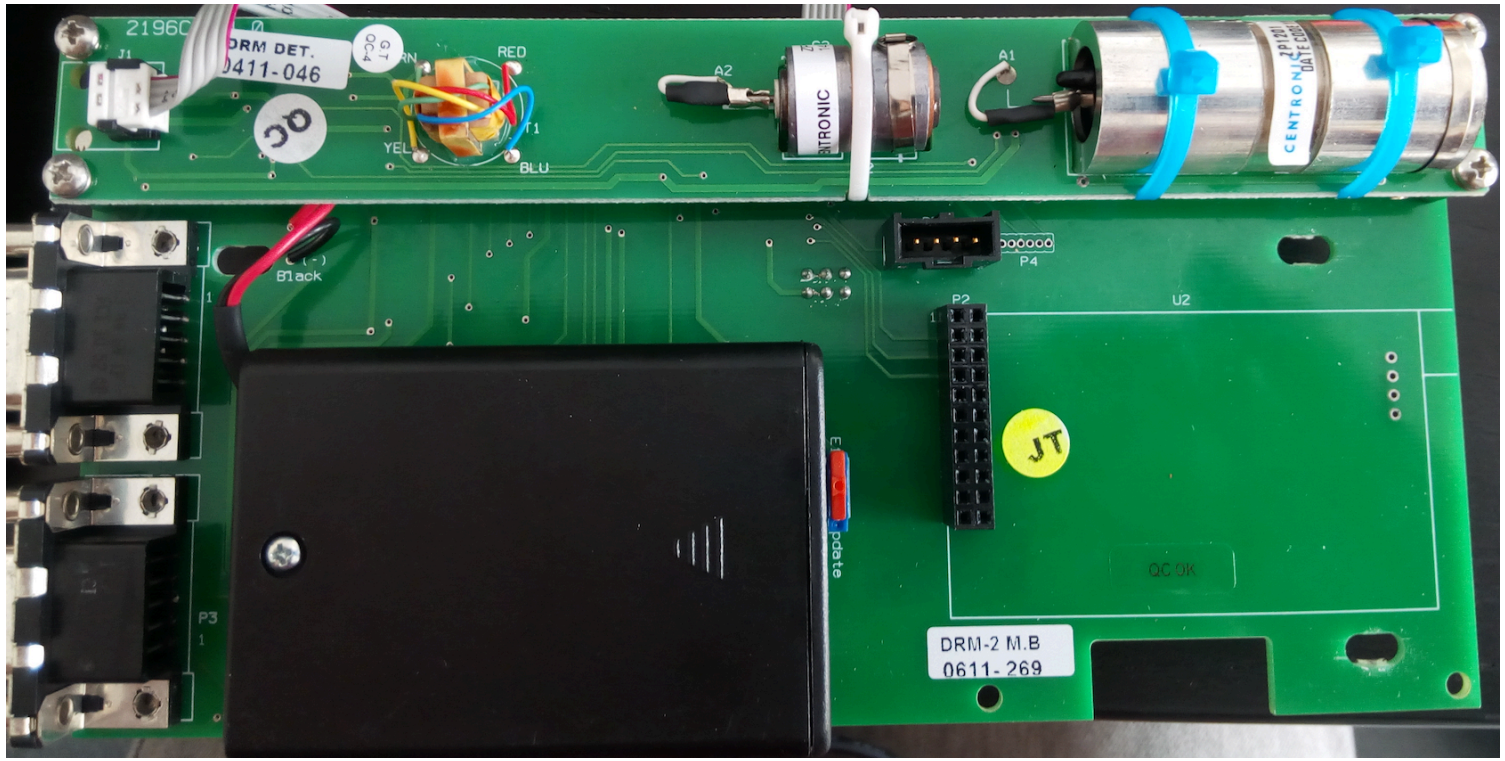
External Transceiver

RAMSYS TX

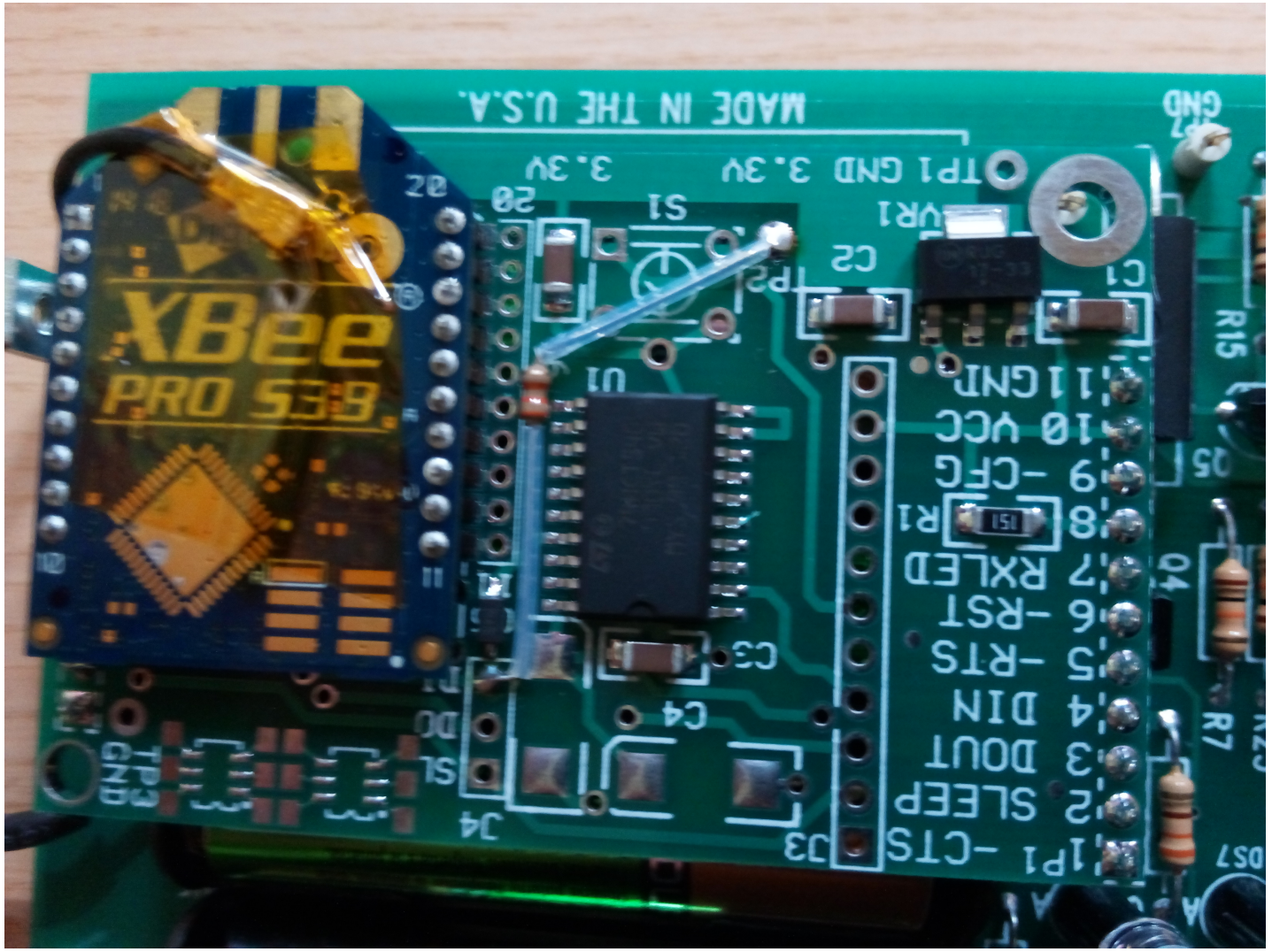
DRM-2


DRM-2
MGP

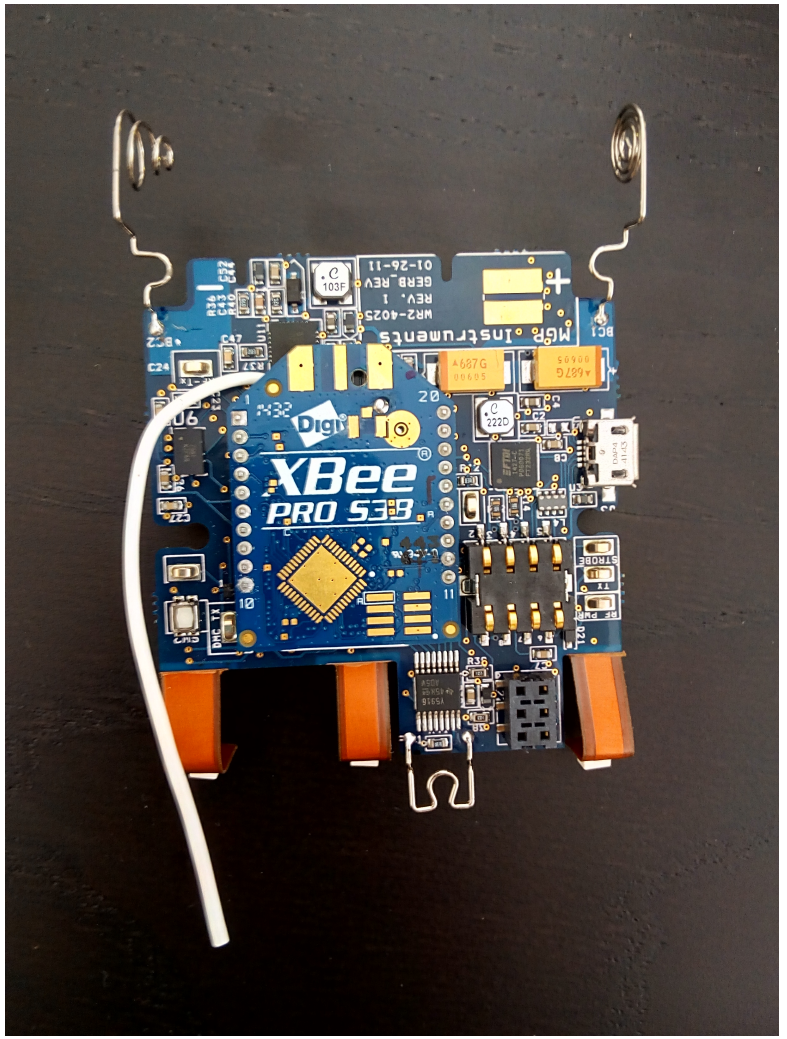

XBee
PRO S3B
2344 CS
V1.2


DRM DET.
0411-046
RED
YEL
BLU
Black
P4
P2
U2
P3
JT
QC OK
DRM-2 M.B
0611-269

Base Transceiver



IPAM-Tx



Digi Xbee-PRO XSC

"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

OEM Range: 0x8000 – 0xFFFF Read-only

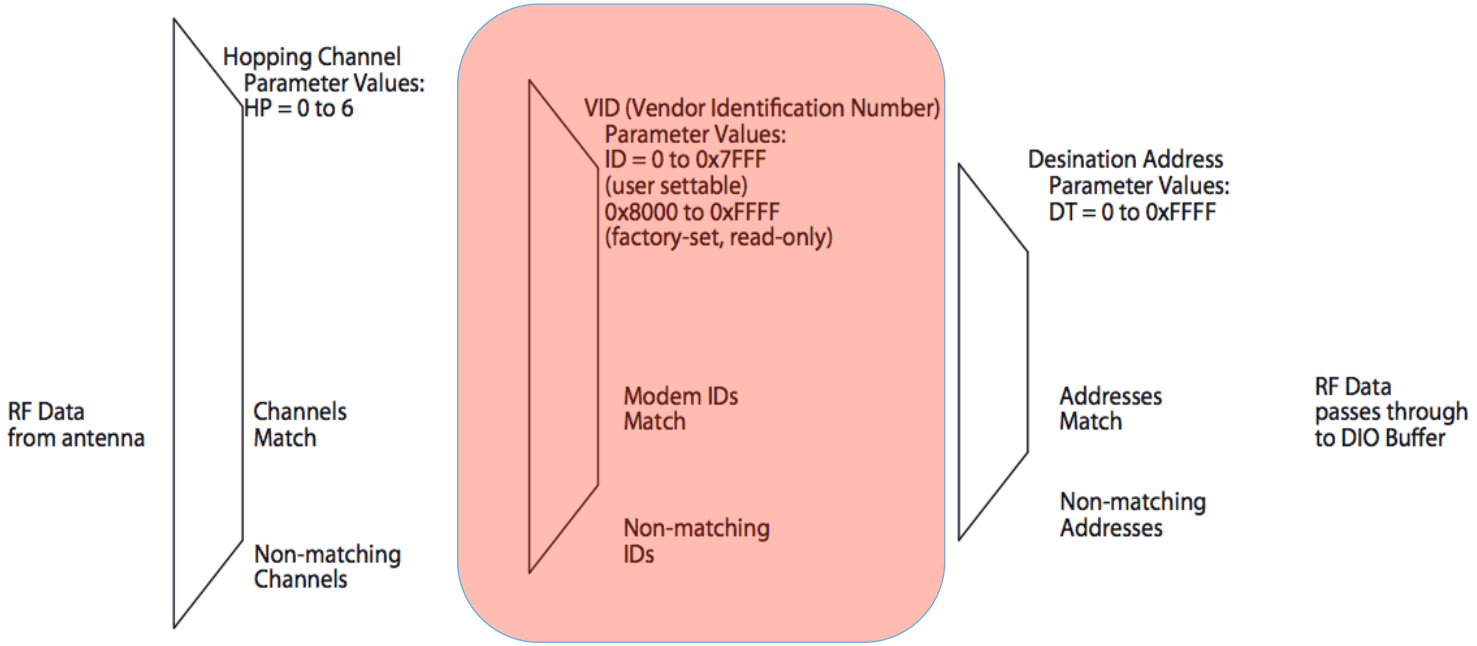
ID	0x27 (39d)	Module VID	User set table: 0x10 - 0x7FFF Read-only: 0x8000 – 0xFFFF	Networking	2	-

OEM networks are 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



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

Goals

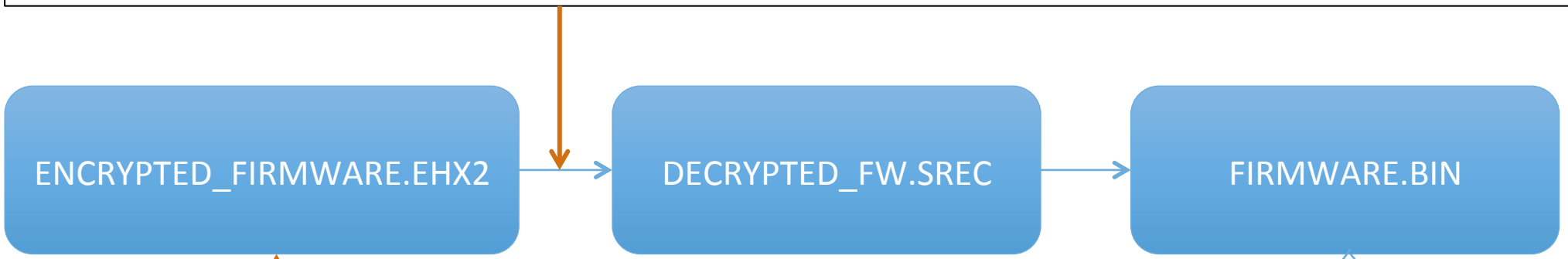
1. Access to arbitrary Digi XSC Networks
2. XSC/WRM2 Analysis

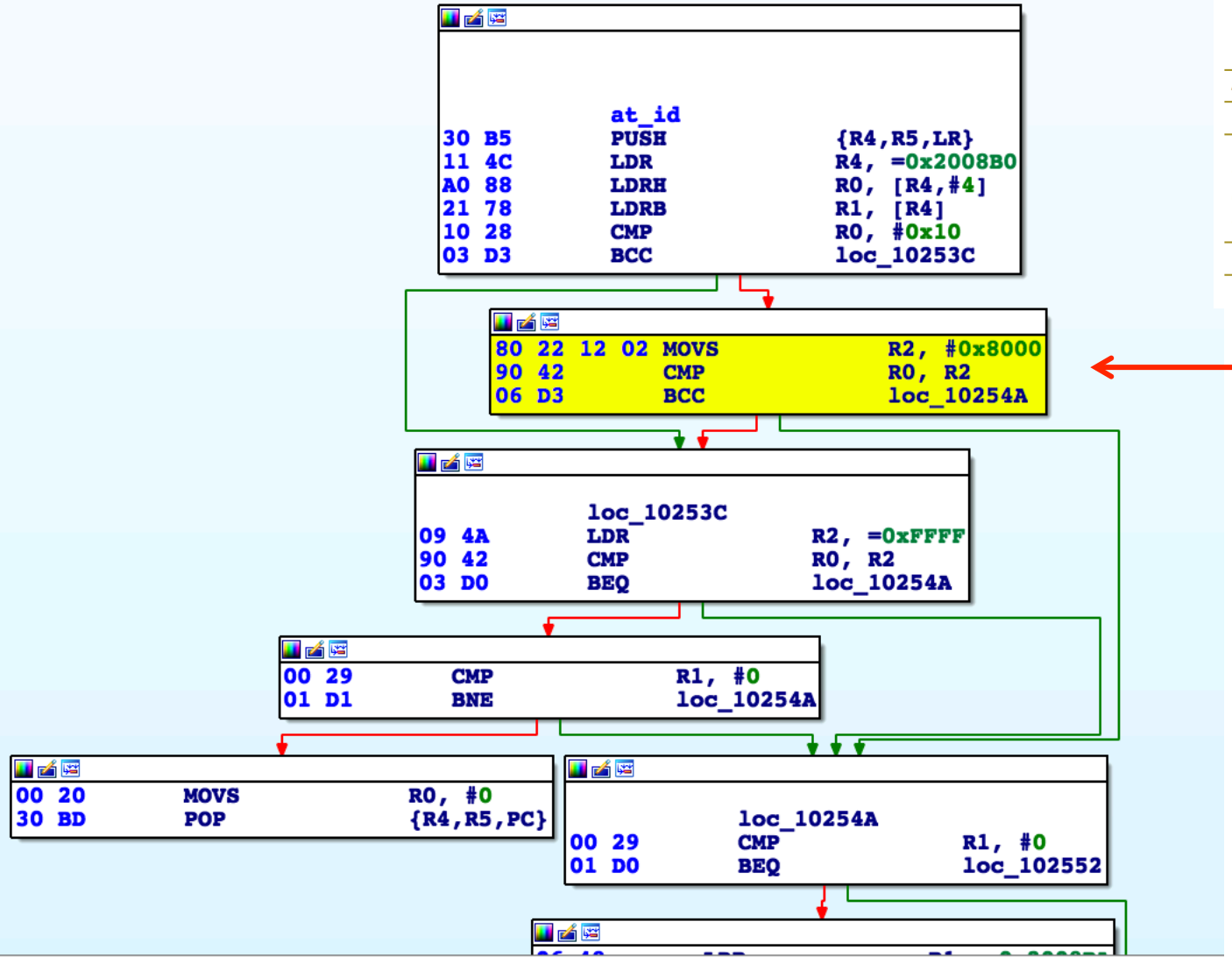
Approach

1. Firmware
2. Hardware
3. Radio

FIRMWARE

```
key = "B7E648AE72434579B7F4D482587075D2B7E648AE72434579".decode('hex')
iv = "B7E648AE72434579".decode('hex')
des3 = DES3.new(key,DES3.MODE_CBC,iv)
```



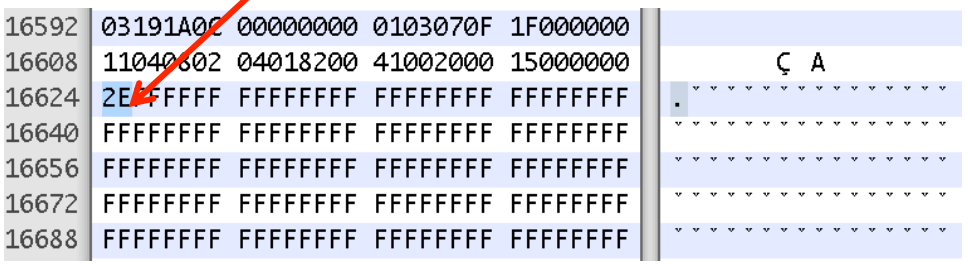


ID (Modem VID) Command

Command Summary	Description
AT Command: ATID	<Networking> Set/Read the "Vendor Identification Number". Only modems with matching IDs can communicate with each other. Modules with non-matching VIDs will not receive unintended data transmission.
Binary Command: 0x27 (39 decimal)	
Parameter Range (user-set table) 0x10 - 0x7FFF (Factory-set and read-only) 0x8000 - 0xFFFF	
Number of bytes returned: 2	

Unlocking OEM Range

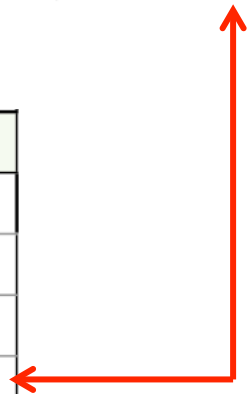
-> Patch + Fix 1-byte Checksum +Encrypt



Hopping Sequences

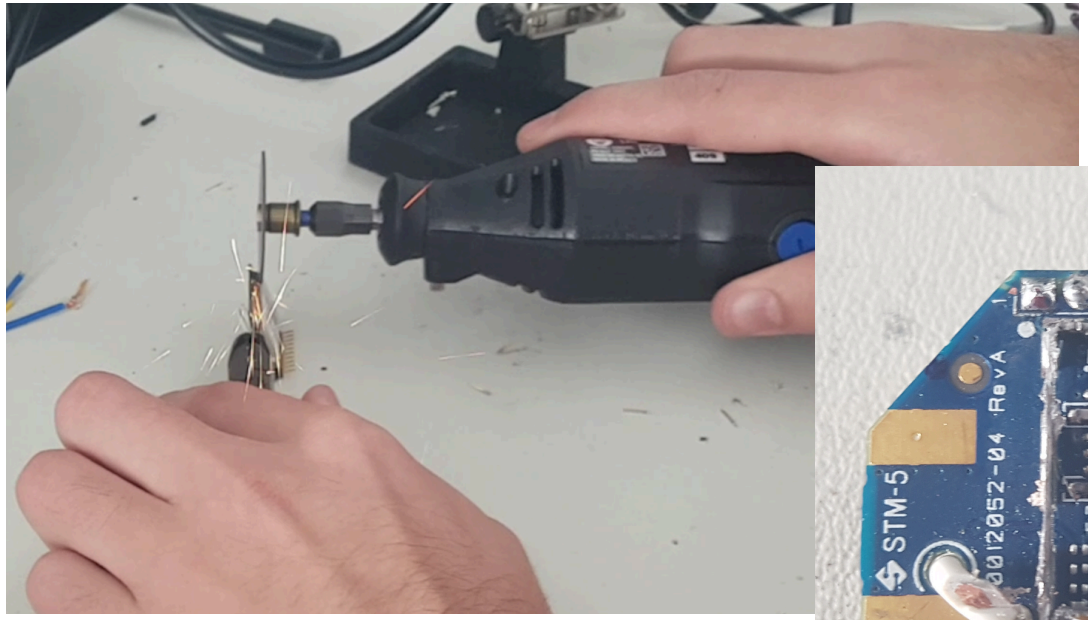
```
ROM:00105010 ; unsigned __int8 patterns[196]
ROM:00105010 patterns        DCB 2, 0x13, 3, 0x12, 0x16, 5, 0x11, 0x10, 9, 0xF, 0xA, 0x17, 0xC, 7, 0xE, 8, 0x14, 0, 6, 0xD, 0xB, 0x15, 1, 0x18, 4; 0
ROM:00105010                                 ; DATA XREF: hopping_pattern+18↑o
ROM:00105010                                 ; ROM:off_102B80↑o
ROM:00105010                 DCB 0x19, 0x1A, 0xC, 5, 3, 0xF, 7, 4, 1, 0x10, 0x17, 0x15, 6, 0x13, 0xD, 0xC, 0xE, 9, 0x12, 0x11, 0x16, 0xA, 0xB, 0, 2; 25
ROM:00105010                 DCB 8, 0x18, 0x14, 0x19, 0x1A, 0xC, 0, 0x18, 0x11, 0x14, 0xC, 7, 4, 0xE, 0xD, 8, 0x12, 0xB, 0x16, 0x13, 2, 9, 0x10, 0x17, 6; 50
ROM:00105010                 DCB 0xF, 0xA, 1, 0x15, 3, 5, 0x19, 0x1A, 0xC, 0xC, 4, 0xB, 0x17, 0x12, 0x11, 2, 8, 0x18, 3, 6, 0x13, 7, 0x10, 0x14, 5; 75
ROM:00105010                 DCB 0, 0x15, 0xE, 0x16, 0xA, 0xF, 0xD, 9, 1, 0x19, 0x1A, 0xC, 0x13, 4, 0xA, 0, 1, 0x18, 0x11, 8, 0x12, 2, 5, 0x10, 0x16; 100
ROM:00105010                 DCB 0xF, 0xE, 9, 6, 0x17, 3, 0xB, 0xD, 0xC, 0x14, 0x15, 7, 0x19, 0x1A, 0xC, 4, 0xE, 0xF, 0xD, 0x18, 0xB, 0x11, 0xC, 3, 7; 125
ROM:00105010                 DCB 0x12, 0x15, 0x17, 0x16, 1, 0x14, 5, 2, 9, 0xA, 0x10, 0x13, 0, 6, 8, 0x19, 0x1A, 0xC, 8, 0x11, 0xD, 0xA, 2, 0, 0x14; 150
ROM:00105010                 DCB 0xB, 6, 0x17, 9, 1, 7, 0x13, 0x12, 0xF, 0xE, 0x16, 0xC, 0x10, 0x15, 5, 4, 0x18, 3, 0x19, 0x1A, 0xC; 175
```

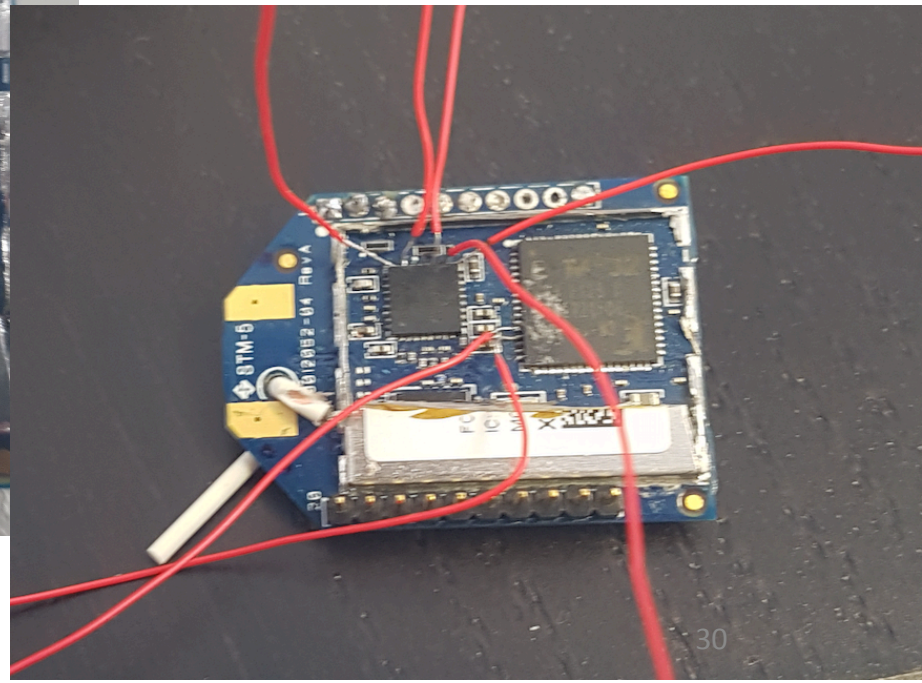
General	
Frequency Range	902-928MHz (located in the 900MHz ISM Band)
Spread Spectrum	Frequency Hopping
Network Topology	Point-to-Point, Peer-to-Peer, Point-to-Multipoint
Channel Capacity	7 hop sequences share 25 frequencies



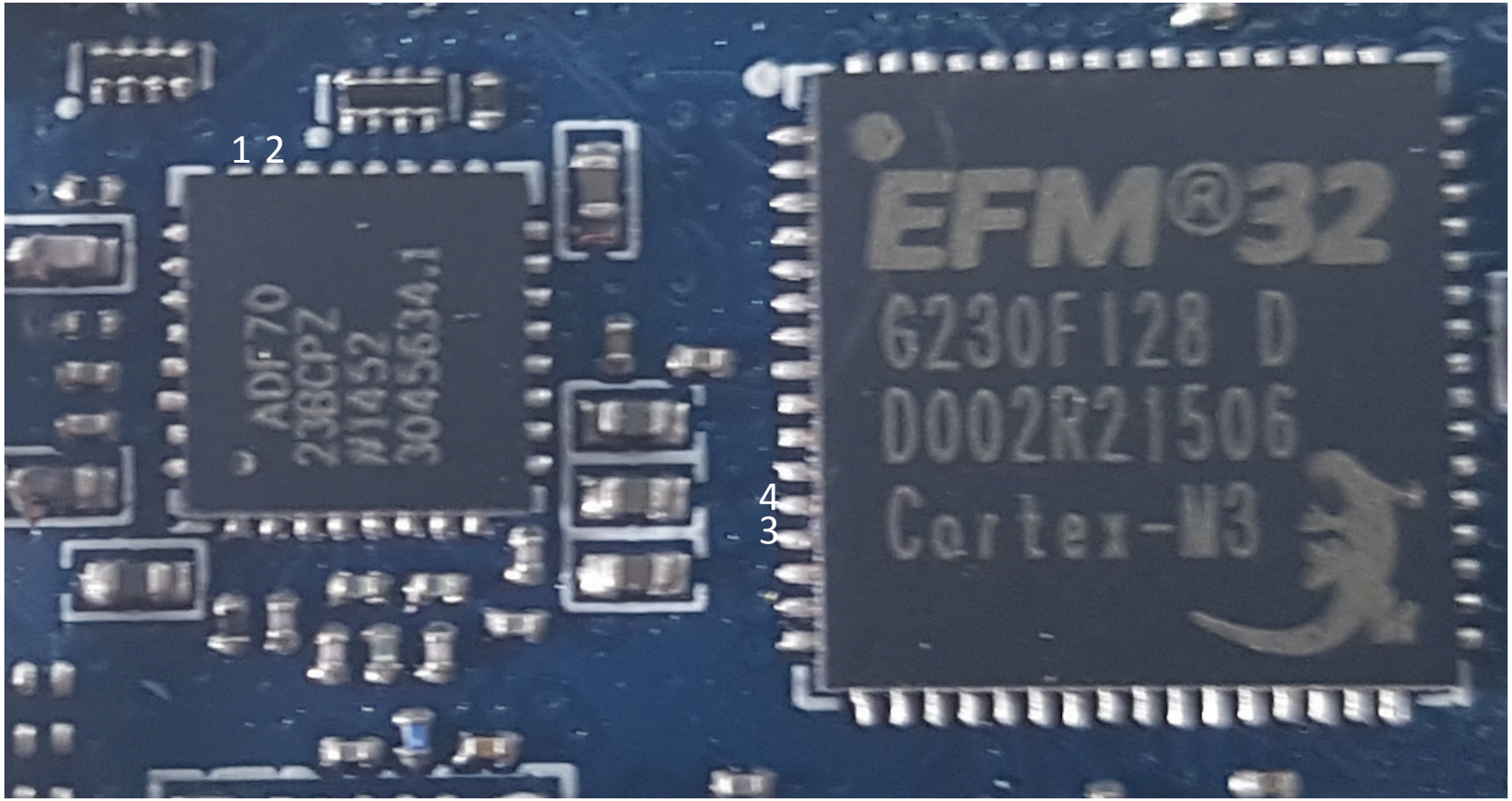
1. Access to arbitrary Digi XSC Networks 
2. XSC/WRM2 Analysis

HARDWARE





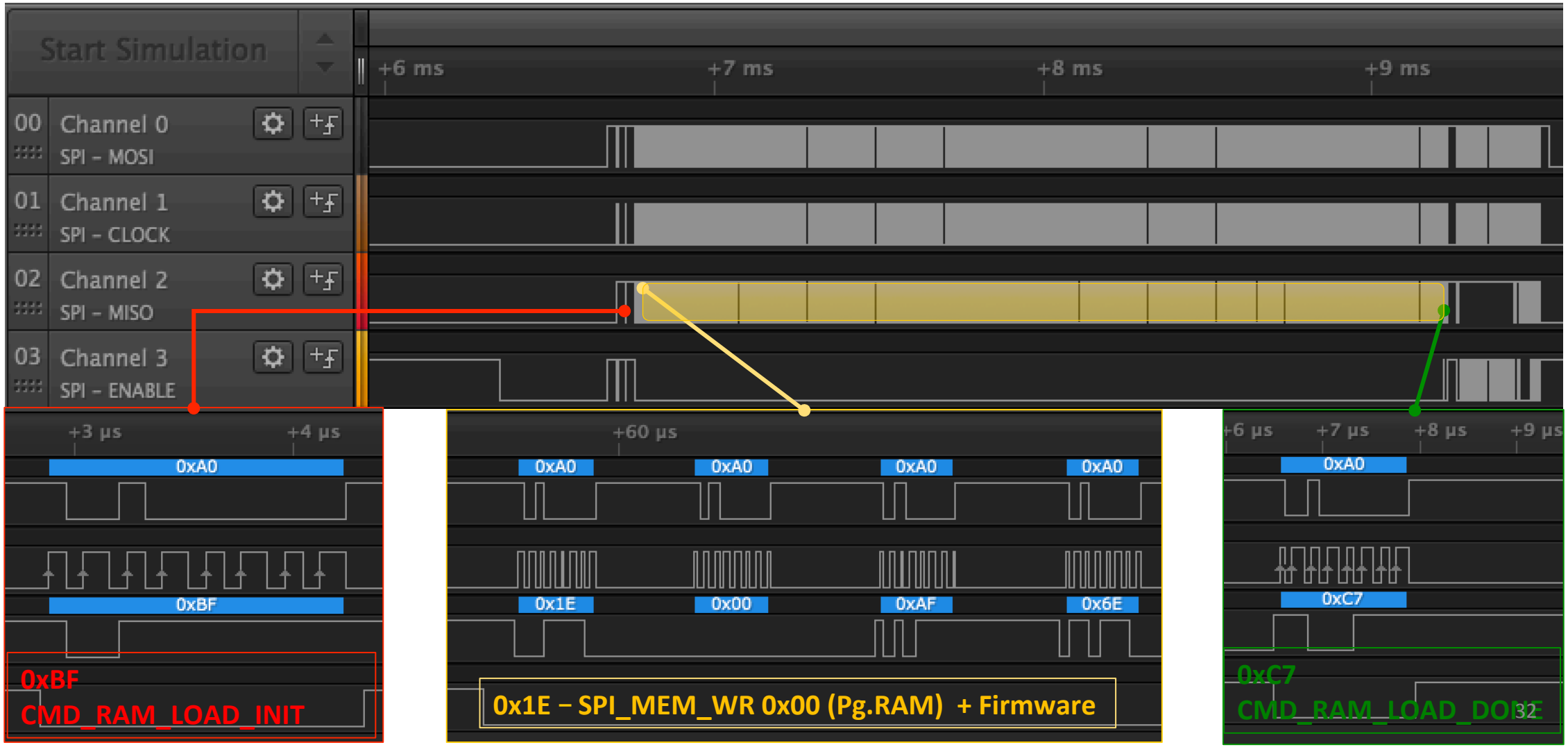
1



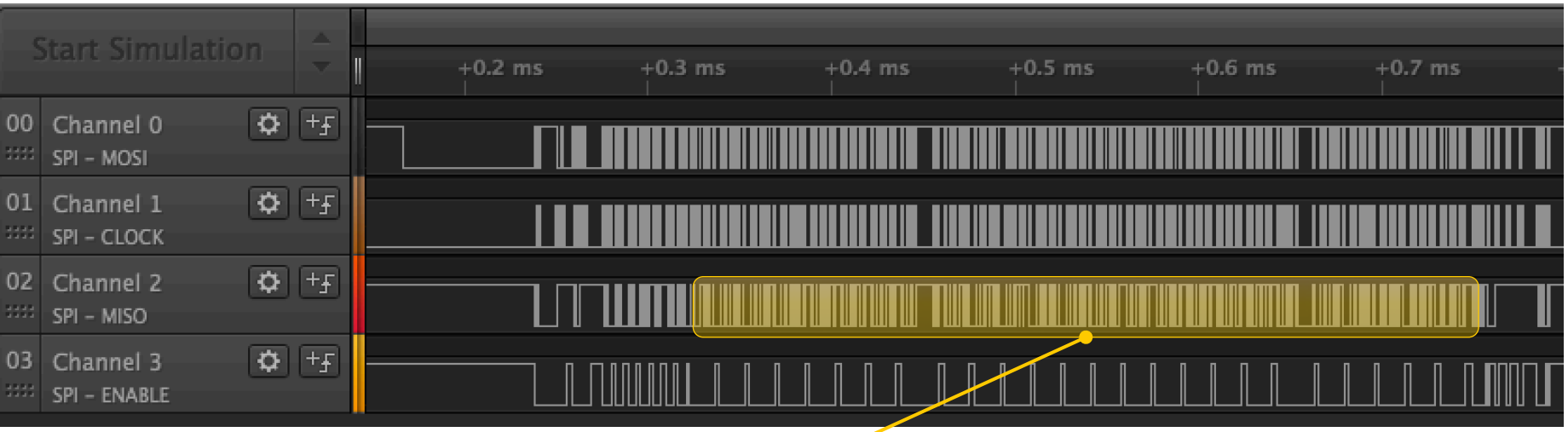
ADF7023

http://www.analog.com/media/en/technical-documentation/data-sheets/ADF7023.pdf

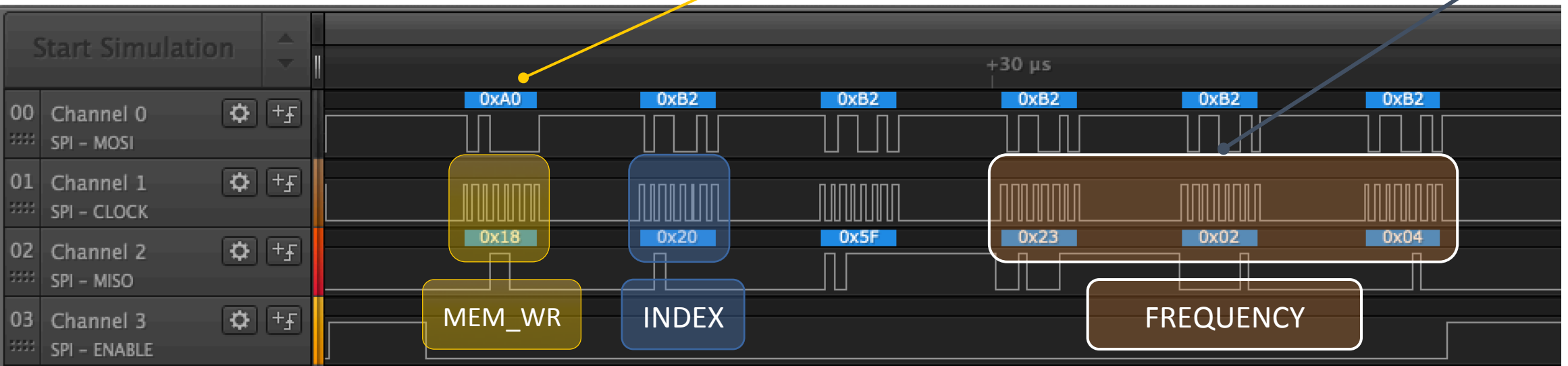
Reset


Start Simulation
+6 ms
+7 ms
+8 ms
+9 ms
00 Channel 0
SPI – MOSI
01 Channel 1
SPI – CLOCK
02 Channel 2
SPI – MISO
03 Channel 3
SPI – ENABLE
+3 µs
+4 µs
0xA0
0xBF
0xBF
CMD_RAM_LOAD_INIT
+60 µs
0xA0
0xA0
0xA0
0xA0
0x1E
0x00
0xAF
0x6E
0x1E – SPI_MEM_WR 0x00 (Pg.RAM) + Firmware
+6 µs
+7 µs
+8 µs
+9 µs
0xA0
0xC7
0xC7
CMD_RAM_LOAD_DONE

Reset



Freq = (26M * Freq_Int)/2^16



Mirion always uses the first Hopping Pattern (0)

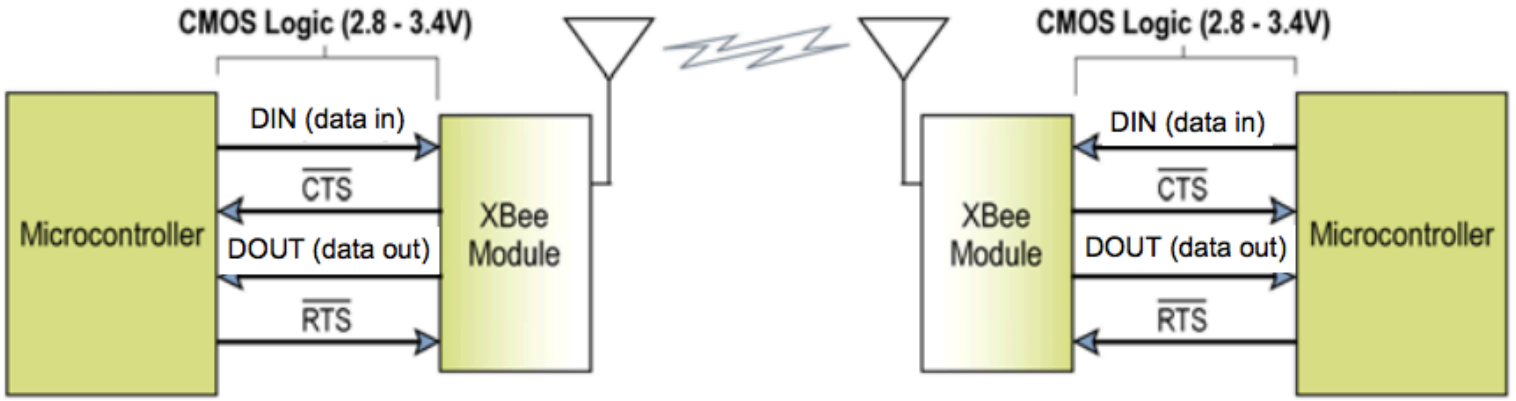
Center Frequencies – Pattern 0 – 25 channels – Digi XSC-PRO	
0. 910518532,1	D. 914418829,6
1. 910818463,4	E. 914718761
2. 911118791,5	F. 915018692,3
3. 911418722,8	10. 915318623,6
4. 911718654,2	11. 915618555
5. 912018585,5	12. 915918883
6. 912318516,8	13. 916218814,4
7. 912618844,9	14. 916518745,7
8. 912918776,2	15. 916818677
9. 913218707,6	16. 917118608,4
A. 913518638,9	17. 917418936,4
B. 913818570,2	18. 917719264,4
C. 914118898,3	

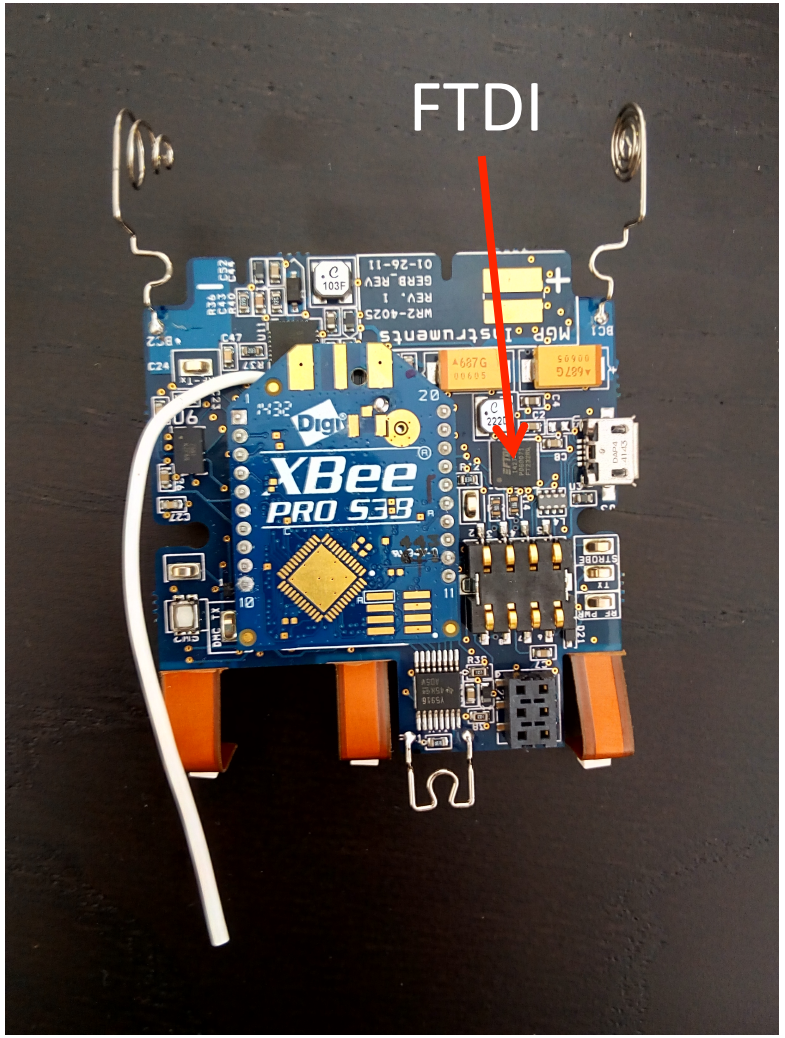
Pattern 0: 2, 0x13, 3, 0x12, 0x16, 5, 0x11, 0x10, 9, 0xF, 0xA, 0x17, 0xC, 7, 0xE, 8, 0x14, 0, 6, 0xD, 0xB, 0x15, 1, 0x18, 4

2.1.1. UART-Interfaced Data Flow

Devices that have a UART interface can connect directly through the pins of the XBee module as shown in the figure below.

Figure 2-01. System Data Flow Diagram in a UART-interfaced environment (Low-asserted signals distinguished with horizontal line over signal name.)



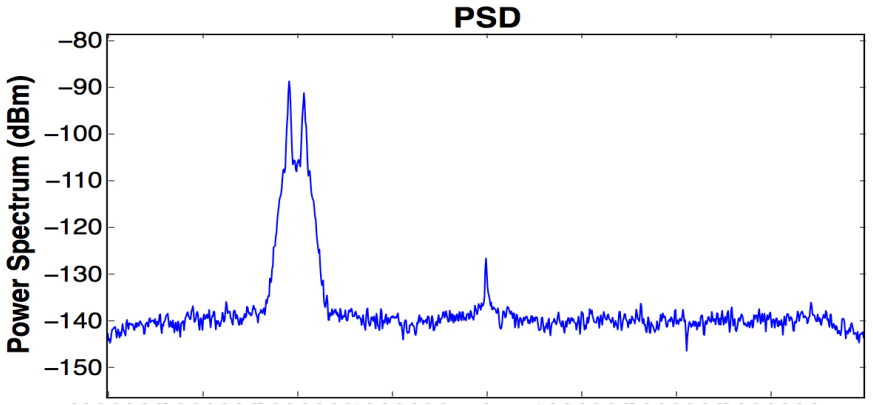


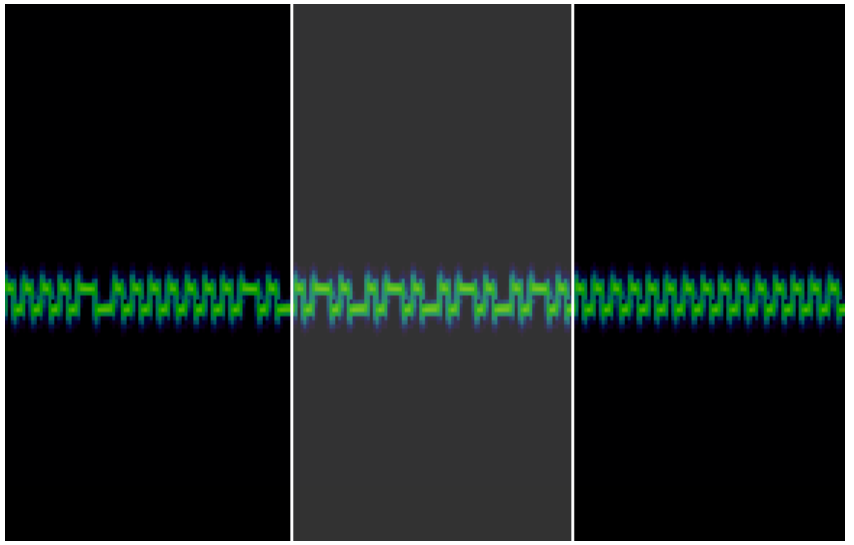
ID + Payload + Checksum

WRM2 Example: 1234567800000000001030YY

RADIO

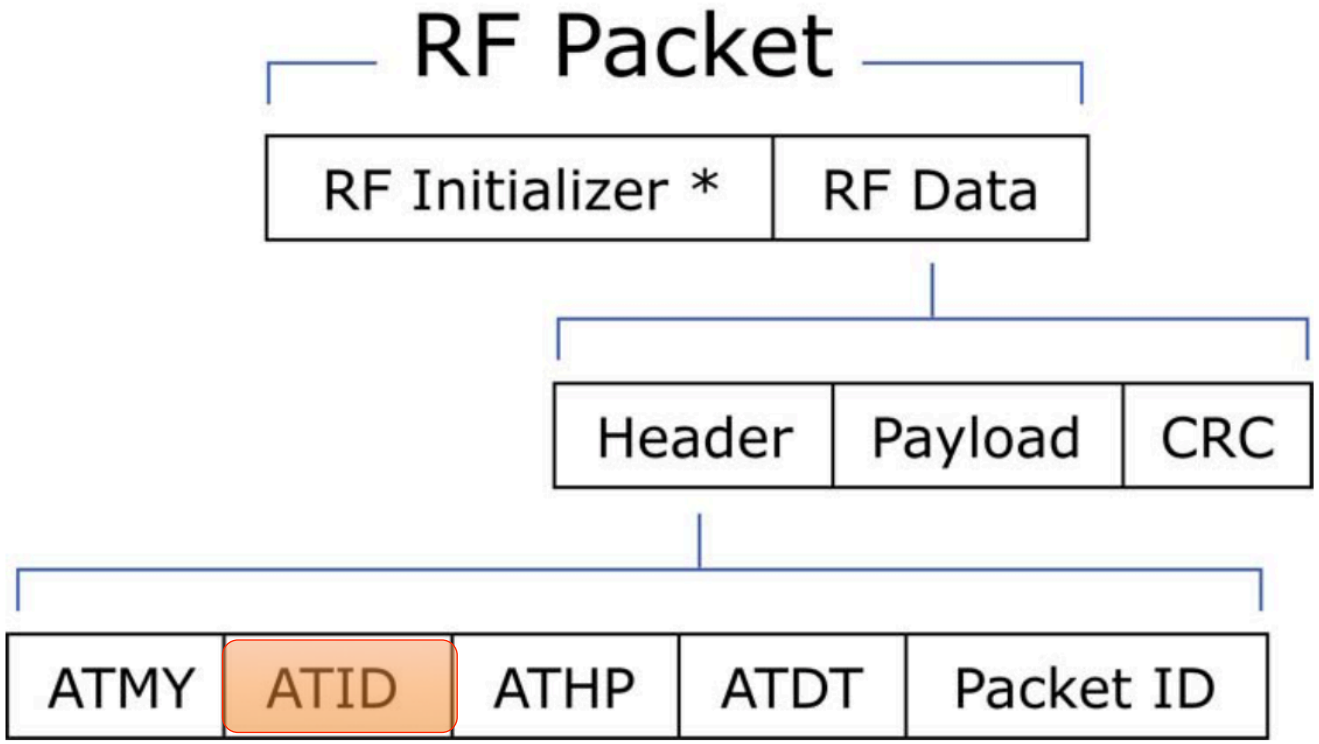
- Modulation
  - 2GFSK
- Encoding Scheme
  - Biphase-S
- FHSS (Slow)
  - Channels
    - Center Frequency
    - Mark
    - Space
    - Width
  - Dwell time
  - Blanking time





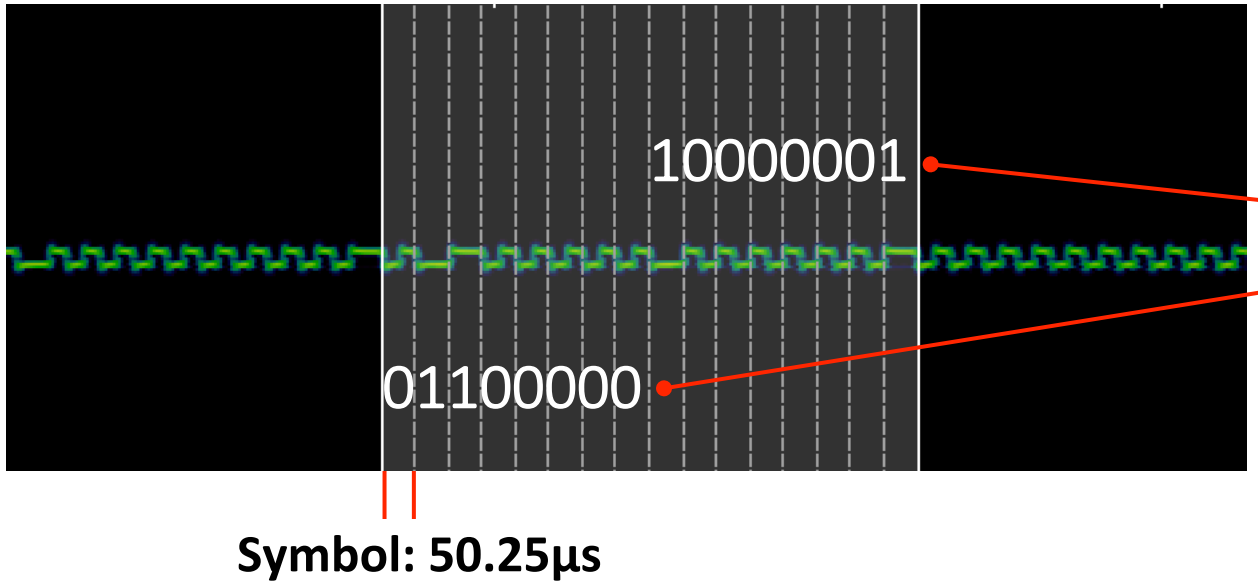
RF Packet

The RF packet is the sequence of data used for communicating information between Digi Radios. An RF Packet consists of an RF Initializer and RF Data.



https://www.digi.com/support/productdetail?pid=5298

Data Encoding



Mirion Network ID: 8160h

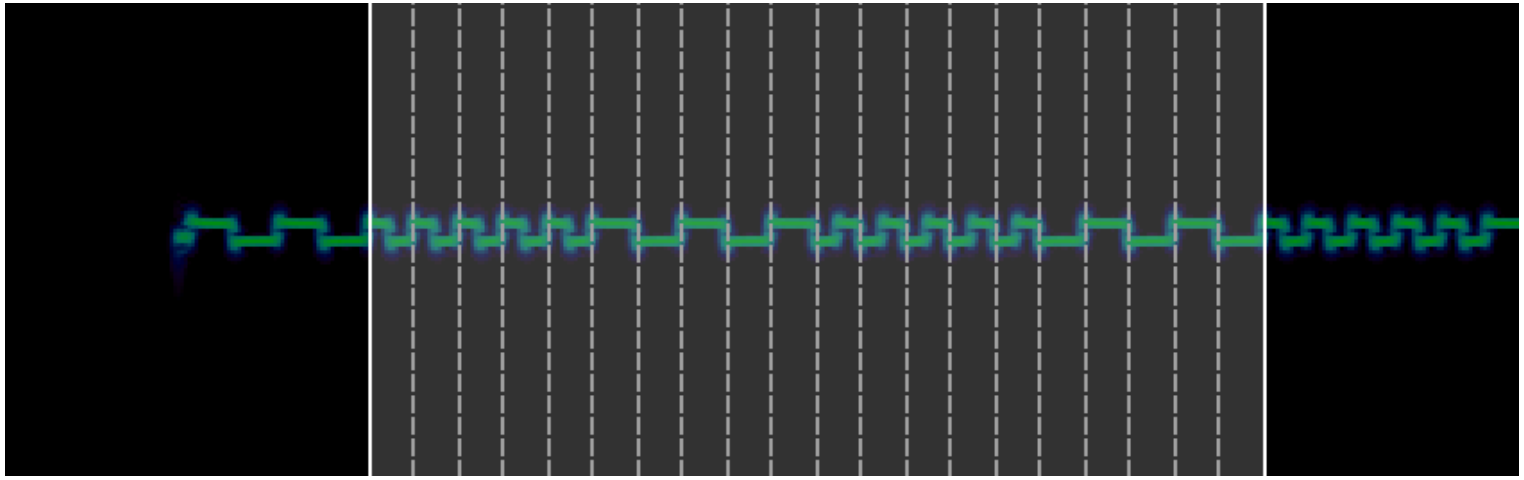
81h = 1000 0001

60h = 0110 0000

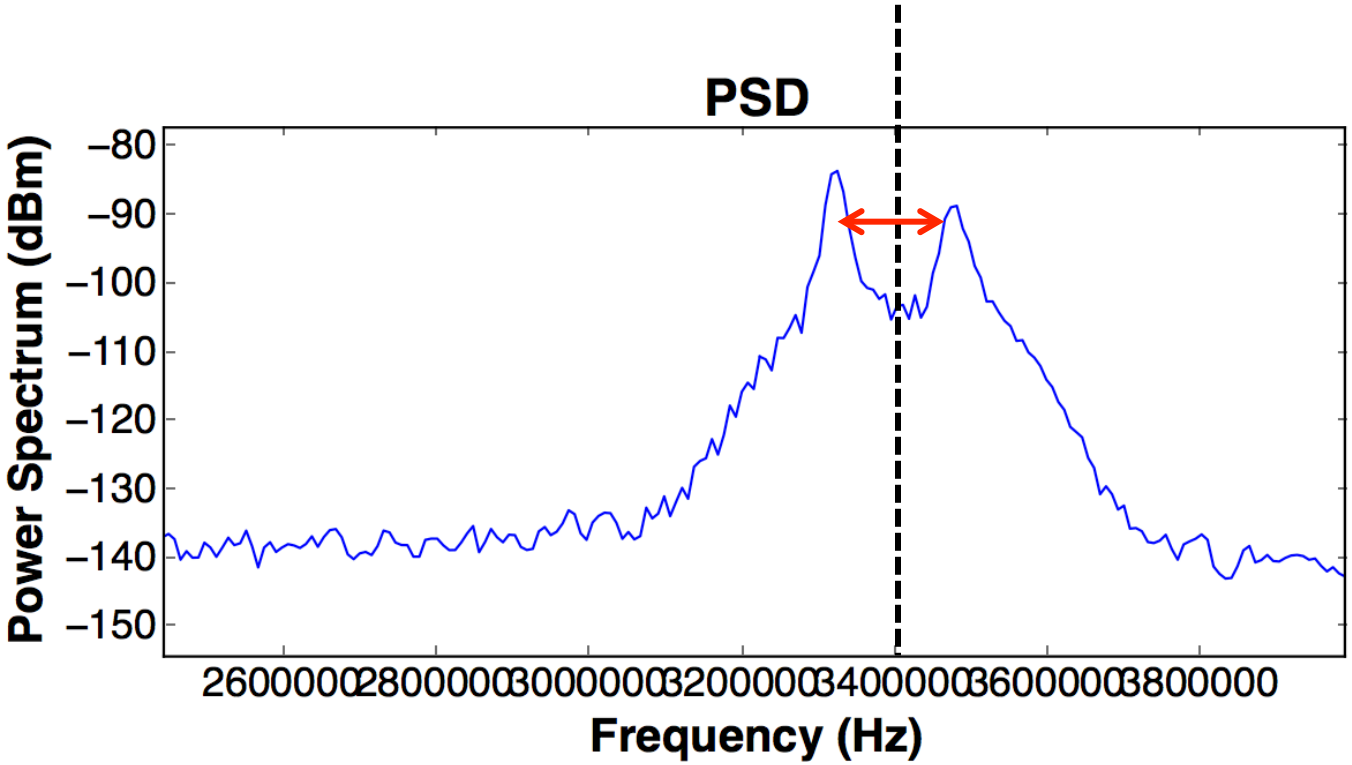
Biphase - Space

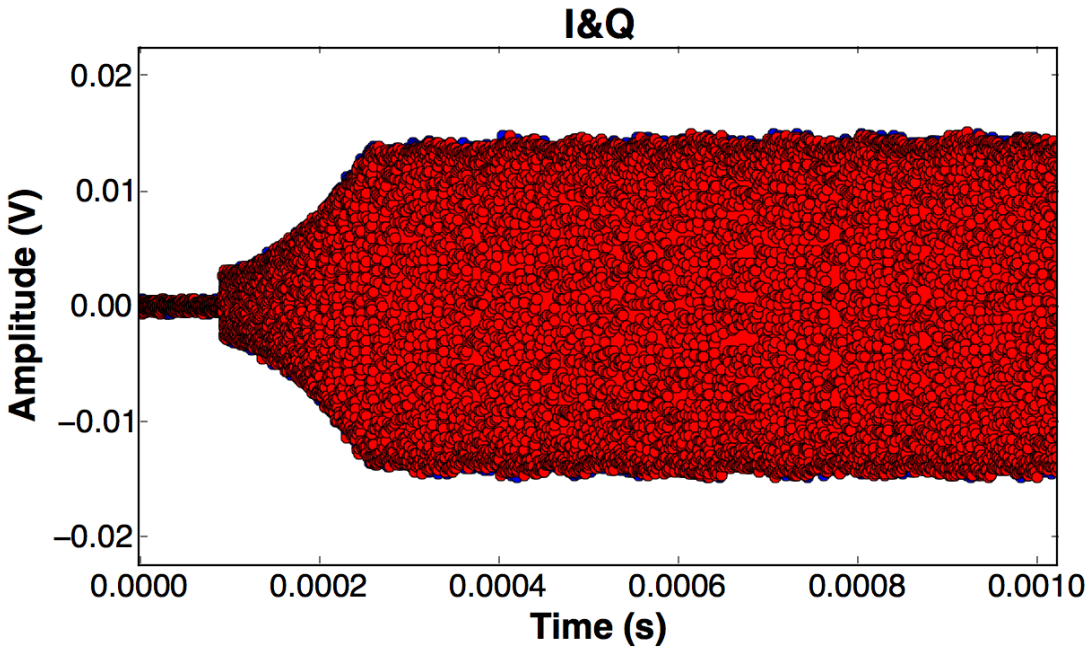
- The signal level changes at the start of every bit time.
- The signal level changes in the middle of a bit time if the bit is 0

Channels



- All channels have the same ‘preamble’
- Each channel has a different ‘Sync Word’


PSD
Power Spectrum (dBm)
−80
−90
−100
−110
−120
−130
−140
−150
2600000
2800000
3000000
3200000
3400000
3600000
3800000
Frequency (Hz)


I&Q
Amplitude (V)
0.02
0.01
0.00
−0.01
−0.02
0.0000
0.0002
0.0004
0.0006
0.0008
0.0010
Time (s)

```
[+] 16000000 samples loaded

IOActive RF Utils - Plugin BlackHat'17 FHSS/2GFSK 0.1 -{Ruben Santamarta}-

Session ======================================
1. Sampling Rate: [ 8000000 Hz ]
2. Block Size: [ 4000 ]
3. Freq Resolution: [ 15625.000 Hz ]
4. Low Freq: [ 910000000.000 Hz ]
5. High Freq: [ 918000000.000 Hz ]

[+] Detecting burst
[*] Found potential signal => Block: 436000 Noise: 0.0001(v) Signal: 0.0125(v)

[+] Detecting Channels...
Channel [0] =>  Center Frequency: 915.0 Mhz     === Offset: [438592 -> 763383]  Time: 0.054500(s) to 0.095000(s)       Span: 0.04050(s) ===
Channel [1] =>  Center Frequency: 913.5 Mhz     === Offset: [1236042 -> 1560903]       Time: 0.154500(s) to 0.195000(s)       Span: 0.04050(s) ===
Channel [2] =>  Center Frequency: 917.4 Mhz     === Offset: [2048946 -> 2373617]       Time: 0.256000(s) to 0.296500(s)       Span: 0.04050(s) ===
Channel [3] =>  Center Frequency: 914.1 Mhz     === Offset: [2843379 -> 3171922]       Time: 0.355000(s) to 0.396000(s)       Span: 0.04100(s) ===
Channel [4] =>  Center Frequency: 912.6 Mhz     === Offset: [3650629 -> 3975441]       Time: 0.456000(s) to 0.496500(s)       Span: 0.04050(s) ===
Channel [5] =>  Center Frequency: 914.7 Mhz     === Offset: [4451519 -> 4776345]       Time: 0.556000(s) to 0.597000(s)       Span: 0.04100(s) ===
Channel [6] =>  Center Frequency: 912.9 Mhz     === Offset: [5259009 -> 5583879]       Time: 0.657000(s) to 0.697500(s)       Span: 0.04050(s) ===
Channel [7] =>  Center Frequency: 916.5 Mhz     === Offset: [6054847 -> 6379668]       Time: 0.756500(s) to 0.797000(s)       Span: 0.04050(s) ===
Channel [8] =>  Center Frequency: 910.5 Mhz     === Offset: [6860663 -> 7185581]       Time: 0.857500(s) to 0.898000(s)       Span: 0.04050(s) ===
Channel [9] =>  Center Frequency: 912.3 Mhz     === Offset: [7663576 -> 7988433]       Time: 0.957500(s) to 0.998500(s)       Span: 0.04100(s) ===
Channel [10] => Center Frequency: 914.4 Mhz     === Offset: [8464460 -> 8789235]       Time: 1.058000(s) to 1.098500(s)       Span: 0.04050(s) ===
Channel [11] => Center Frequency: 913.8 Mhz     === Offset: [9273564 -> 9598462]       Time: 1.159000(s) to 1.199500(s)       Span: 0.04050(s) ===
Channel [12] => Center Frequency: 916.7 Mhz     === Offset: [10071130 -> 10395934]     Time: 1.258500(s) to 1.299000(s)       Span: 0.04050(s) ===
Channel [13] => Center Frequency: 910.8 Mhz     === Offset: [10880439 -> 11205313]     Time: 1.360000(s) to 1.400500(s)       Span: 0.04050(s) ===
Channel [14] => Center Frequency: 917.7 Mhz     === Offset: [11678376 -> 12002881]     Time: 1.459500(s) to 1.500000(s)       Span: 0.04050(s) ===
Channel [15] => Center Frequency: 911.7 Mhz     === Offset: [12486012 -> 12810807]     Time: 1.560500(s) to 1.601000(s)       Span: 0.04050(s) ===
Channel [16] => Center Frequency: 911.1 Mhz     === Offset: [13285129 -> 13609978]     Time: 1.660500(s) to 1.701000(s)       Span: 0.04050(s) ===
Channel [17] => Center Frequency: 916.3 Mhz     === Offset: [14087701 -> 14412515]     Time: 1.760500(s) to 1.801500(s)       Span: 0.04100(s) ===
Channel [18] => Center Frequency: 911.4 Mhz     === Offset: [14891781 -> 15216722]     Time: 1.861000(s) to 1.902000(s)       Span: 0.04100(s) ===

[+] Done.
```

1. Access to arbitrary Digi XSC Networks ✓
2. XSC/WRM2 Analysis ✓

ATTACK SCENARIOS

‘Radioactive Leak’ Attack

OSINT

Emergency Action Levels

Annex 1: Unit 1 **V. C. Summer Nuclear Station**

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*

Virgil C. Summer Power Plant (US) Emergency Plan https://www.nrc.gov/docs/ML1104/ML110410260.pdf

[powernet] Question regarding number WRM Base Transceivers

Kinmark, Michael J | Tue, 12 Apr 2016 12:54:53 -0700

Question from Columbia regarding utilities using Mirion (MGPI) Wireless Remote Monitoring equipment.

1) What number of WRM2 Base Transceiver (WR2-9001) Units do you have deployed out in the plant (outage and non-outage - if different)?

2) How many WRM2 Base Transceiver units vs. WRM2 Repeater units?

We are currently evaluating our system needs and have 5 WRM2 Base Transceivers in service with 2 stand-alone units on mobile carts.

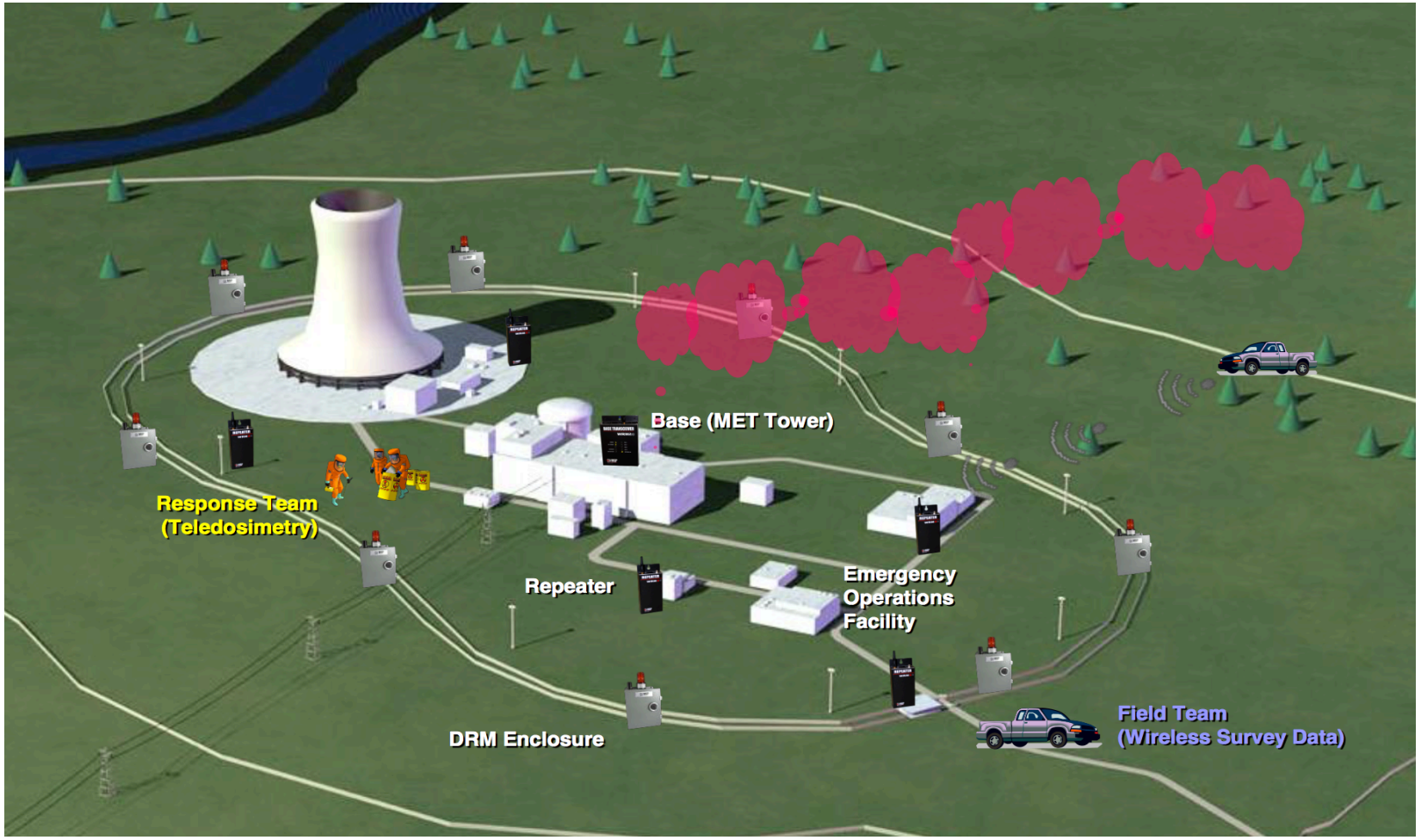
Thank you in advance.

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

V.C. Summer NPP – Auxiliary Building Roof

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

'Sabotaging Health Physics/Emergency Response Teams' Attack



- Failed Evacuation
- Concealed Persistent Attack

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

Responsible Disclosure

- ✖ **Ludlum** **June, 2014**
- ✖ **Digi** **May, 2017**
- ✖ **Mirion** **May, 2017**

Thank you!