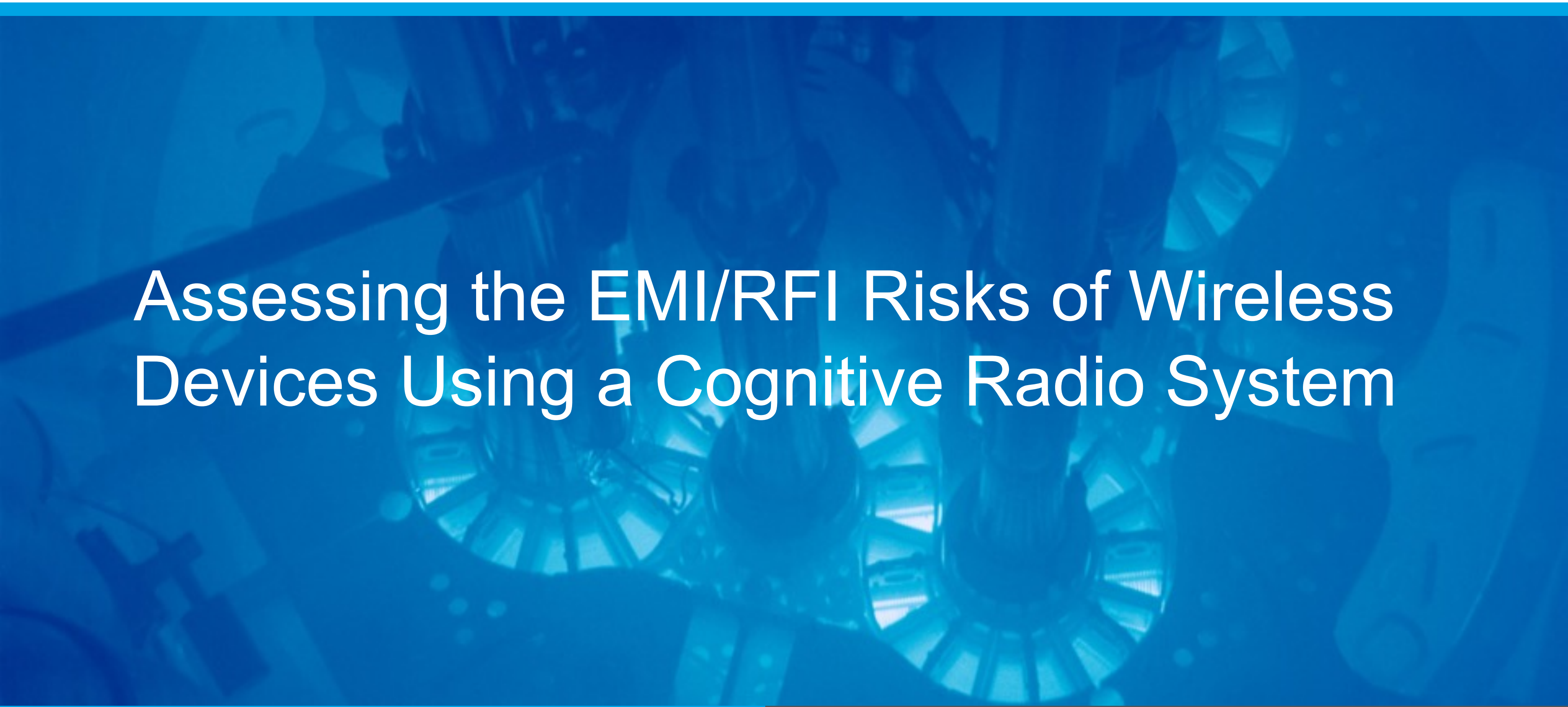


Assessing the EMI/RFI Risks of Wireless Devices Using a Cognitive Radio System

Advanced Sensors and Instrumentation Annual Webinar

October 31 – November 1, 2018

Chad Kiger

AMS Corporation

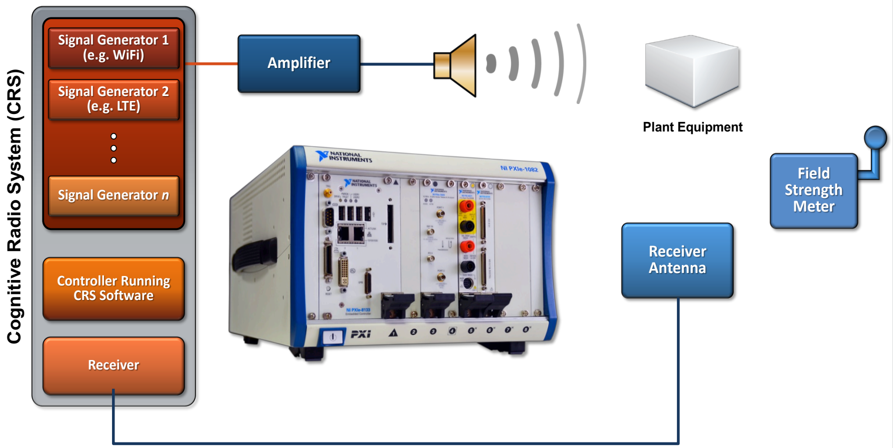
SBIR Phase I/II

Strategy for Implementation of Fixed and Mobile Wireless Technologies in Crowded and Confined EMI Environments of Nuclear Power Plants

Chad Kiger/ Analysis and Measurement Services Corporation

Technology Summary

The goal of the Phase II project was to develop a system that establishes objective exclusion distances for safe and widespread use of wireless devices in nuclear power plants. Referred to as a Cognitive Radio System (CRS), the product of this project is a light-weight portable unit that can be carried around a plant to test for radiated immunity and wireless co-existence. It can transmit and receive electromagnetic waves to establish distances at which existing plant equipment will not be affected by wireless signals and that multiple wireless devices in the same area will not interfere with each other.


Cognitive Radio System (CRS)
Signal Generator 1 (e.g. WiFi)
Signal Generator 2 (e.g. LTE)
Signal Generator n
Controller Running CRS Software
Receiver
Amplifier
Plant Equipment
Field Strength Meter
Receiver Antenna

Key Personnel

Chad Kiger, Chris Lowe, Zack Crane, Brad Headrick, Keith Ryan, Josh Cole, Jonathan Caughron, Mehrad Hashemian, Ryan O'Hagan

Program Summary

Period of Performance:

Start Date: 6/9/2014 End Date: 7/27/2018

Key Milestones & Deliverables	
Year 1 Phase I	• Evaluate equipment to wireless vulnerabilities • Develop test method to assess immunity of equipment
Year 2 Phase II	• Define the requirements of CRS • Design and build CRS
Years 3 & 4 Phase II	• Test and Validate CRS • Implement CRS in nuclear power plants

Technology Impact

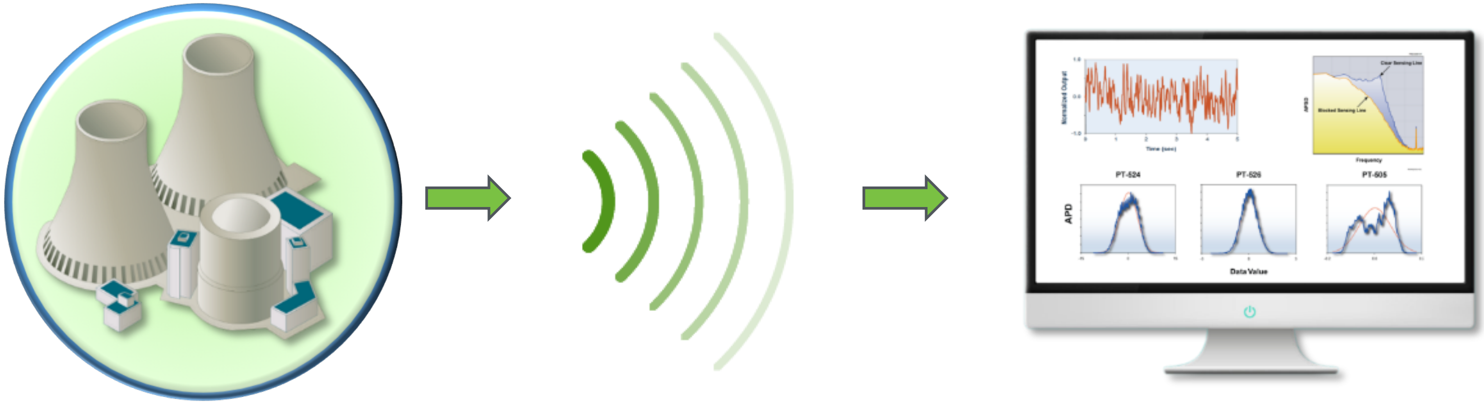
This technology offers to make the usage of wireless devices a possibility in that exclusion distances in almost all nuclear power plants are still overly conservative and thereby severely limit the use of wireless devices in most areas of the plant. Studies have shown that the usage of wireless devices in an nuclear power plant increases efficiency gains which leads to cost savings.

Support the Implementation of Wireless Technologies into Nuclear Power Plants

Desire to use Wireless in the Nuclear Industry

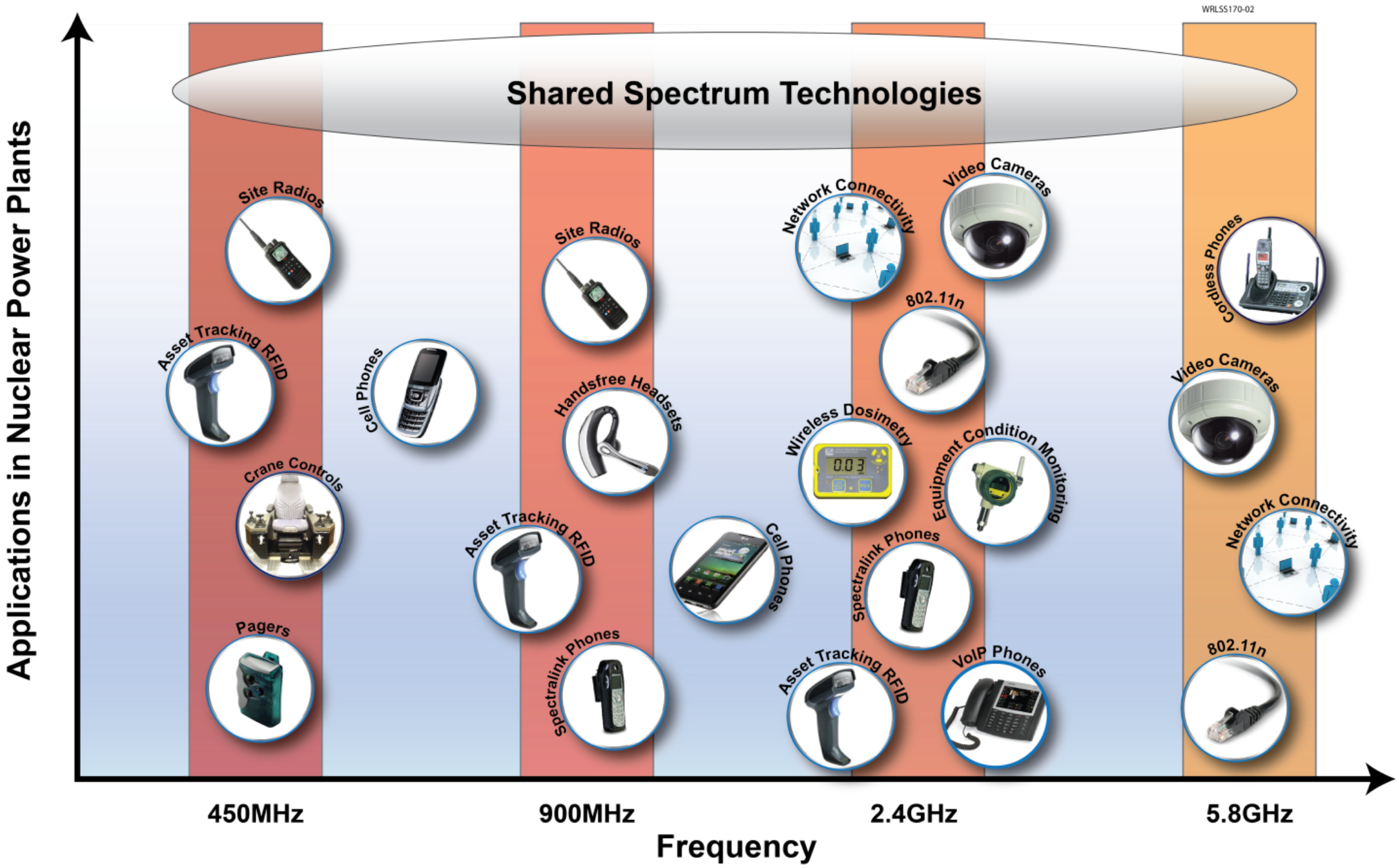
The Mobile, Digital Worker

Use of Wireless Devices in Power Plants



Data Accessibility, Communications, Equipment Condition Monitoring

Wireless Technology limited to Several Different Frequency Bands



Exclusion Zones were Developed to Prevent EMI/RFI

- Exclusion zone distances depend on transmitter power and antenna gain
- Can be overly conservative and restrictive
- **Does NOT account for Frequency**

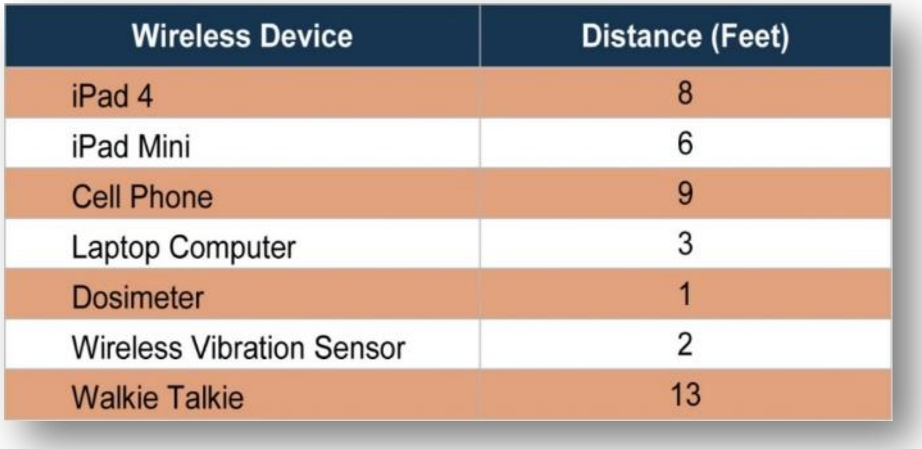
$$d = \frac{\sqrt{30 P_t G_t}}{E} (meters)$$

Where:
$d =$ *exclusion zone distance (in meters);*

$P_t =$ *the effective radiated power of the EMI/RFI emitter (in Watts);*

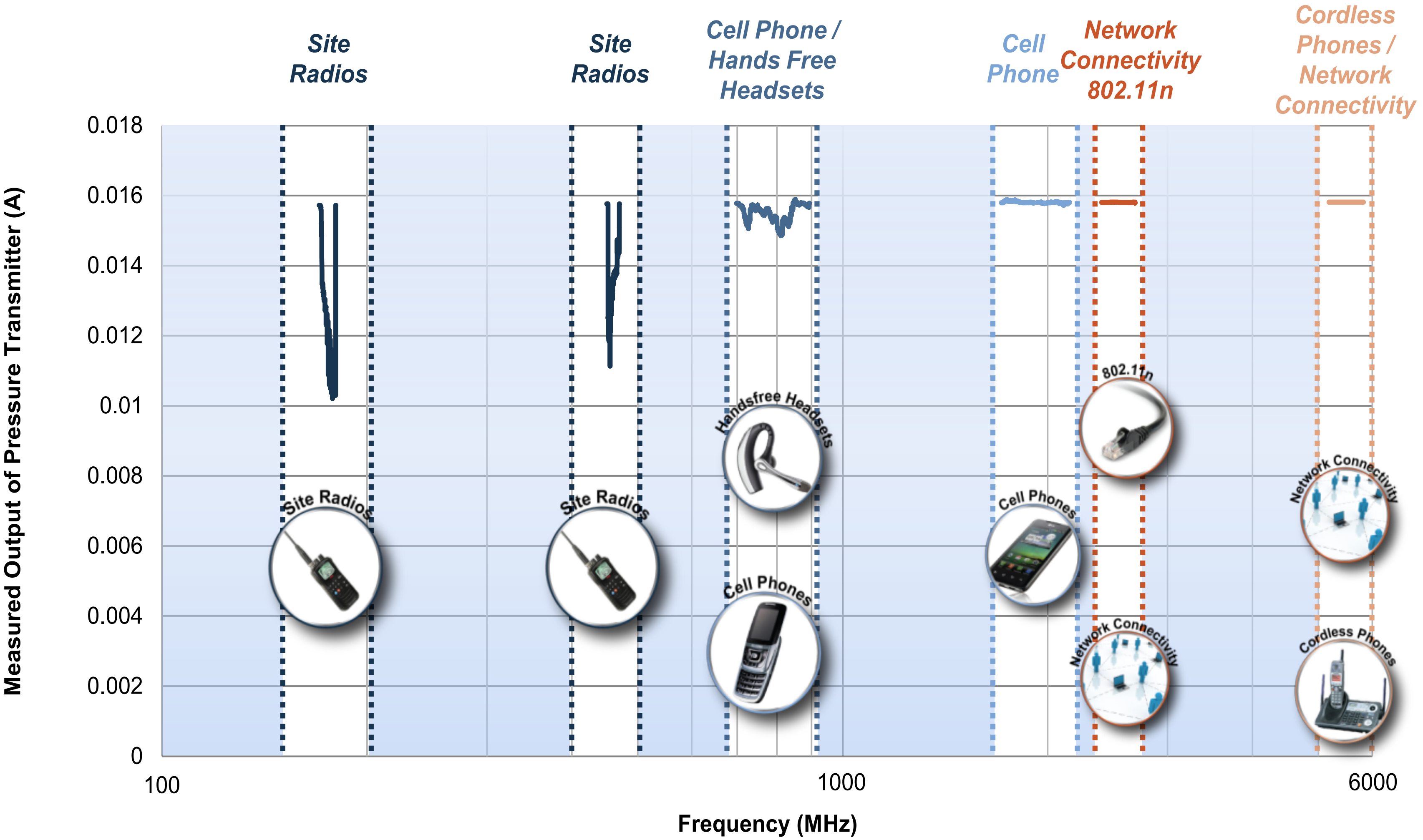
$G_t =$ *the gain of the EMI/RFI emitter (dimensionless);and,*

$E =$ *the allowable radiated electric field strength of the EMI/RFI emitter (in Volts/meter).*

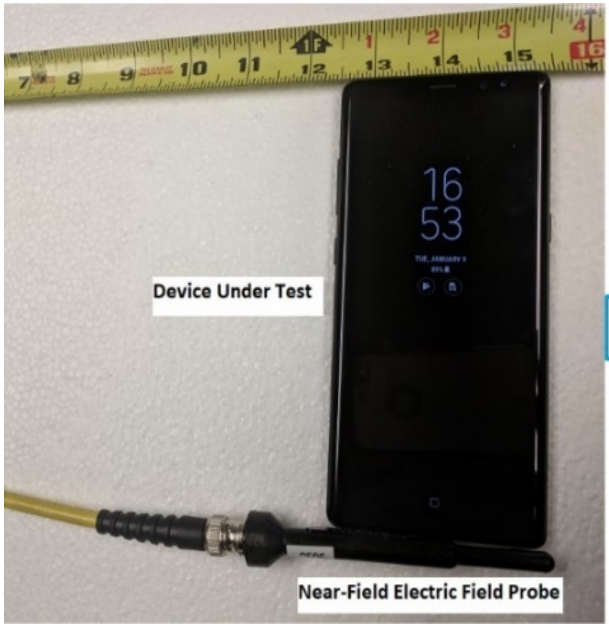


Wireless Device	Distance (Feet)
iPad 4	8
iPad Mini	6
Cell Phone	9
Laptop Computer	3
Dosimeter	1
Wireless Vibration Sensor	2
Walkie Talkie	13

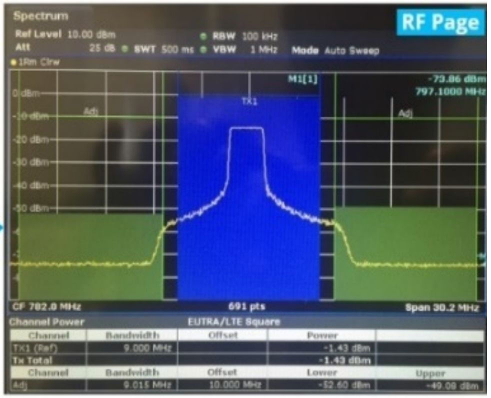
Vulnerabilities Identified in a Pressure Transmitter are FREQUENCY Dependent



Wireless signals are not replicated during EMC Qualification Testing



Span of 300 MHz



Spectrum

Ref Level 10.00 dBm RBW 100 kHz

Att 25 dB SWT 500 ms VBW 1 MHz Mode Auto Sweep

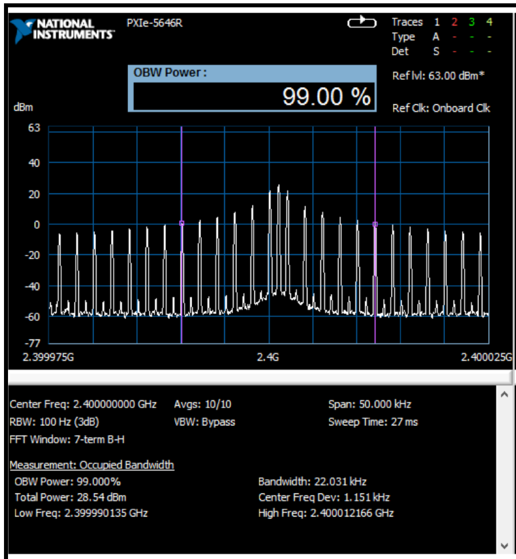
M1[1] -73.86 dBm 797.1000 MHz

CF 782.0 MHz 691 pts Span 30.2 MHz

Channel Power EUTRA/LTE Square

Channel	Bandwidth	Offset	Power	
TX1 (Ref)	9.000 MHz		-1.43 dBm	
Tx Total			-1.43 dBm	
Channel	Bandwidth	Offset	Lower	Upper
Adj	9.015 MHz	10.000 MHz	-52.60 dBm	-49.08 dBm

Span of 50 kHz



Center Freq: 2.400000000 GHz Avgs: 10/10 Span: 50.000 kHz

RBW: 100 Hz (3dB) VBW: Bypass Sweep Time: 27 ms

FFT Window: 7-term B-H

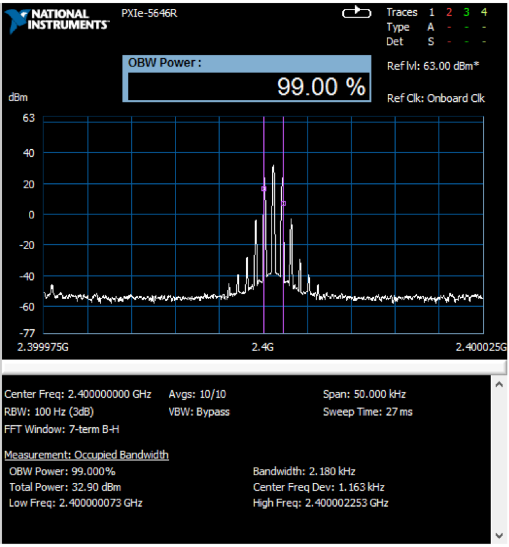
Measurement: Occupied Bandwidth

OBW Power: 99.000% Bandwidth: 22.031 kHz

Total Power: 28.54 dBm Center Freq Dev: 1.151 kHz

Low Freq: 2.399990135 GHz High Freq: 2.400012166 GHz

PM, 50% Duty, 1 kHz @ 2.4 GHz



Center Freq: 2.400000000 GHz Avgs: 10/10 Span: 50.000 kHz

RBW: 100 Hz (3dB) VBW: Bypass Sweep Time: 27 ms

FFT Window: 7-term B-H

Measurement: Occupied Bandwidth

OBW Power: 99.000% Bandwidth: 2.180 kHz

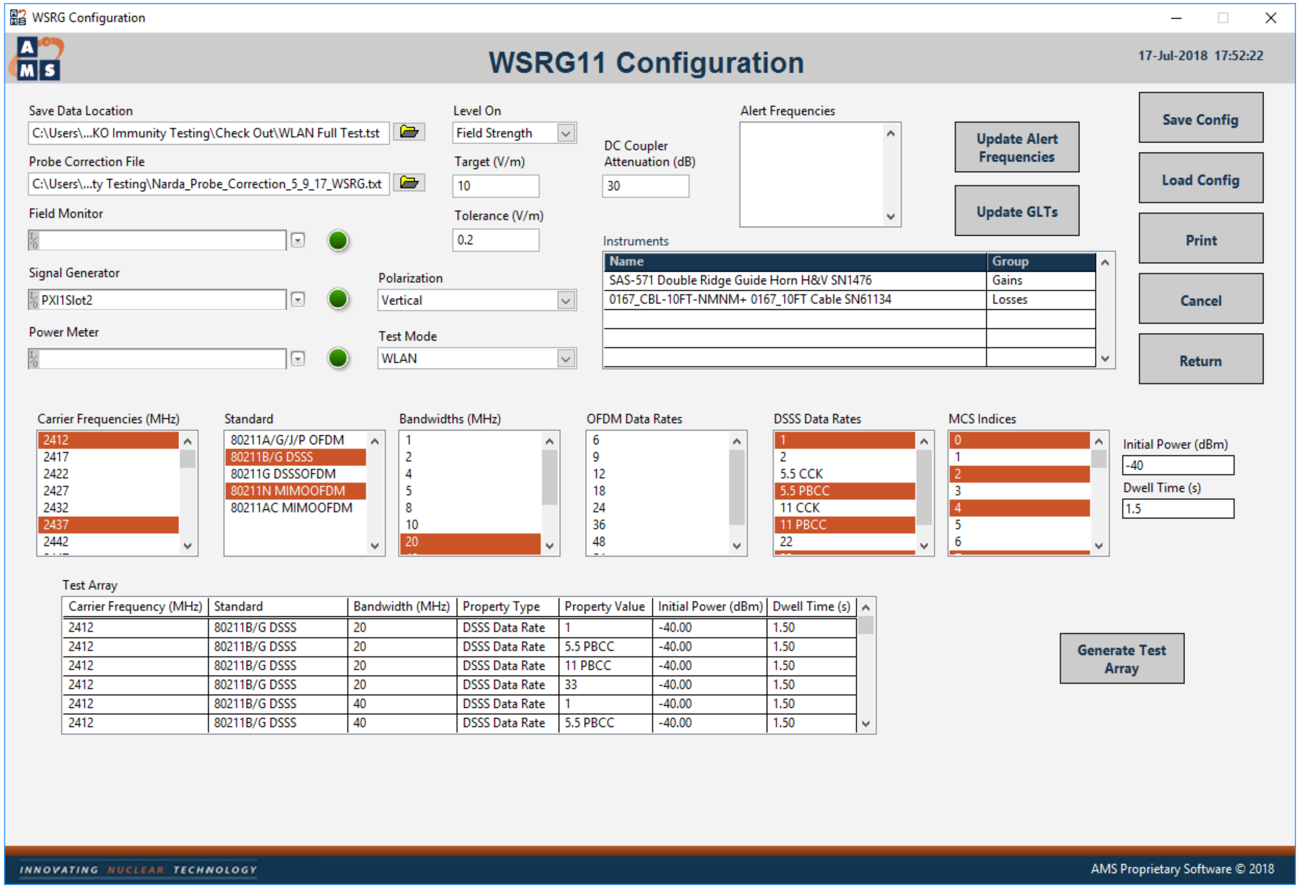
Total Power: 32.90 dBm Center Freq Dev: 1.163 kHz

Low Freq: 2.400000073 GHz High Freq: 2.400002253 GHz

AM, 80%, 1 kHz @ 2.4 GHz

Development of Cognitive Radio System (CRS)

Replicate LTE, Wi-Fi, Bluetooth, DECT, and GSM



WSRG Configuration

WSRG11 Configuration

17-Jul-2018 17:52:22

Save Data Location: C:\Users\...KO Immunity Testing\Check Out\WLAN Full Test.tst

Probe Correction File: C:\Users\...ty Testing\Narda_Probe_Correction_5_9_17_WSRG.txt

Field Monitor:

Signal Generator: PXI1Slot2

Power Meter:

Level On: Field Strength

Target (V/m): 10

Tolerance (V/m): 0.2

Polarization: Vertical

Test Mode: WLAN

DC Coupler Attenuation (dB): 30

Alert Frequencies:

Instruments

Name	Group
SAS-571 Double Ridge Guide Horn H&V SN1476	Gains
0167_CBL-10FT-NMNM+ 0167_10FT Cable SN61134	Losses

Carrier Frequencies (MHz): 2412, 2417, 2422, 2427, 2432, 2437, 2442

Standard: 80211A/G/J/P OFDM, 80211B/G DSSS, 80211G DSSSOFDM, 80211N MIMOOFDM, 80211AC MIMOOFDM

Bandwidths (MHz): 1, 2, 4, 5, 8, 10, 20

OFDM Data Rates: 6, 9, 12, 18, 24, 36, 48

DSSS Data Rates: 1, 2, 5.5 CCK, 5.5 PBCC, 11 CCK, 11 PBCC, 22

MCS Indices: 0, 1, 2, 3, 4, 5, 6

Initial Power (dBm): -40

Dwell Time (s): 1.5

Test Array

Carrier Frequency (MHz)	Standard	Bandwidth (MHz)	Property Type	Property Value	Initial Power (dBm)	Dwell Time (s)
2412	80211B/G DSSS	20	DSSS Data Rate	1	-40.00	1.50
2412	80211B/G DSSS	20	DSSS Data Rate	5.5 PBCC	-40.00	1.50
2412	80211B/G DSSS	20	DSSS Data Rate	11 PBCC	-40.00	1.50
2412	80211B/G DSSS	20	DSSS Data Rate	33	-40.00	1.50
2412	80211B/G DSSS	40	DSSS Data Rate	1	-40.00	1.50
2412	80211B/G DSSS	40	DSSS Data Rate	5.5 PBCC	-40.00	1.50

Method for Reducing Exclusion Distances while Verifying Immunity of Plant Equipment

Address Installed Plant Equipment

1. Site walkdowns to identify equipment that may be vulnerable to wireless signals
2. EMI/RFI mapping to characterize the plant environment
3. In-situ susceptibility testing of plant equipment using standard test methods and actual wireless signals

Other Considerations

1. Laboratory qualification testing of new plant equipment to higher RF levels and using representative wireless signals
2. Laboratory testing of wireless devices to measure their RF emissions and establish objective Exclusion Distances

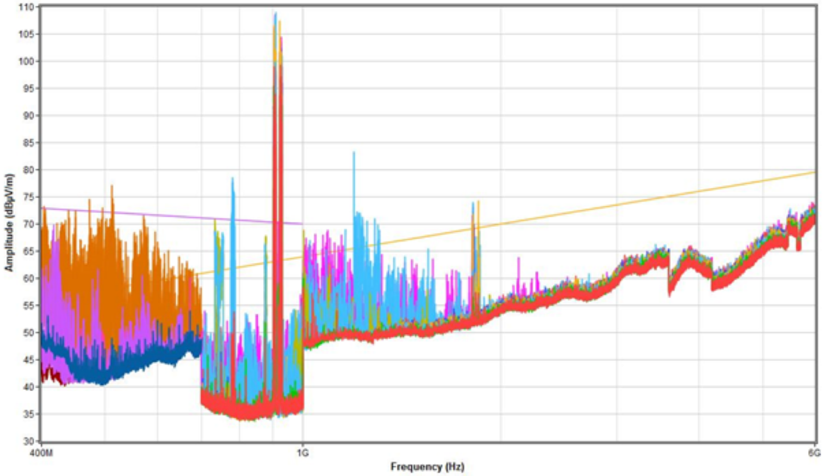
Mapping of Nuclear Power Plants to Characterize the EMI / RFI Environment

- Passive Mapping (RF spectrum monitoring) to characterize environment

- Based on MIL-STD 461 RE102 as recommended by EPRI TR-102323 and NRC Regulatory Guide 1.180

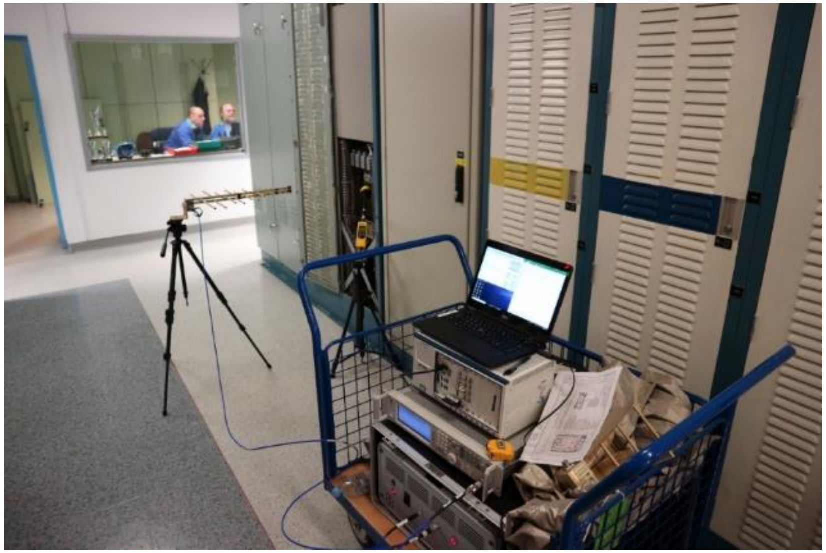
- Identify levels of existing wireless and high frequency signals

- Identify emissions from plant equipment in the frequency range of wireless devices



In-situ Immunity Testing can Identify EMI/RFI Vulnerabilities

- Based on MIL-STD 461 RS103 for frequencies of interest (typically 400 MHz to 6 GHz)
- Software Defined Radio capable of generating representative wireless signals
  - Wi-Fi
  - LTE
  - Bluetooth
  - Others
- Perform testing:
  - In-situ on installed equipment
  - Training center or simulator
  - EMC laboratory
- Mitigate vulnerabilities through additional shielding, filtering, or other means



Clean. **Reliable.** **Nuclear.**