INL/EXT-17-43347-Revision-1

Cyber Security Concerns for Sharing Distributed Antenna Systems

Todd Keller, Luis Quinones, David Kelle, Jacob Benjamin, Arupjyoti Bhuyan, Jason Abrahamson

September 2017

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-17-43347-Revision-1

Cyber Security Concerns for Sharing Distributed Antenna Systems

Todd Keller, Luis Quinones, David Kelle, Jacob Benjamin, Arupjyoti Bhuyan, Jason Abrahamson

September 2017

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy

Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CONTENTS

FIGURES

Cybersecurity Concerns for Sharing Distributed Antenna Systems

1. Executive Summary

Wireless access to data is a challenge for environments with poor radio frequency (RF) coverage such as nuclear power plants. An 802.11 Wi-Fi data network often is not a cost-effective solution due to the extensive antenna outlay requirement for large nuclear facilities and poor signal penetration due to thick concrete walls. Combining commercial Long-Term Evolution (LTE) with an existing distributed antenna system's (DAS) resources and infrastructure is an attractive solution due to lower implementation costs while achieving needed RF coverage. A 2017 technical report by the Electric Power Research Institute (EPRI) demonstrated that multiple systems such as Land Mobile Radio and LTE can be operated sharing the same DAS, leaky coaxial cabling and indoor antenna systems. Since the RF bands used by the two wireless systems are specified to be non-overlapping, it is believed that the systems are isolated from each other. Prior to this project, no extensive analysis had been conducted to determine whether cyber manipulation can enable RF signals from one system to influence another while sharing a DAS, leaky coaxial cable, and antennas. This paper investigates the assumption of isolation between the two wireless systems and provides recommendations for future needed work to identify specific vulnerabilities and potential mitigations.

2. Background

Wireless access to data is a challenge for environments with poor radio frequency (RF) coverage such as nuclear power plants. The 802.11 Wi-Fi data network often is not a cost-effective solution due to the extensive antenna outlay requirement for large nuclear facilities and poor signal penetration due to thick concrete walls. In March 2017, the Electric Power Research Institute (EPRI) released a technical report which investigated the use of Long-Term Evolution (LTE) networks and distributed antenna systems (DASs) to provide RF coverage within nuclear power plants (Reference 1). The study sought to determine the technical feasibility of leveraging an existing DAS infrastructure for LTE in addition to its original use for Land Mobile Radio (LMR) based voice communications.

EPRI demonstrated that 1) multiple systems such as Land Mobile Radio and LTE can be operated successfully using the same DAS, 2) LTE can provide desired data communications inside a nuclear plant with similar RF coverage to the existing LMR system by using the same leaky coaxial cabling and antennas, and 3) commercial 700 MHz LTE systems provide much better RF coverage for data communications than bands with higher frequencies.

3. System Descriptions

The research team chose to use a proposed design modification from a nuclear plant's representative network configuration for this study. The plant's upgrade is based upon the architecture described in the 2017 EPRI technical report. Figure 1 shows the high-level architecture diagram for a communication network architecture that adds wireless data capabilities to its existing wireless voice capability.

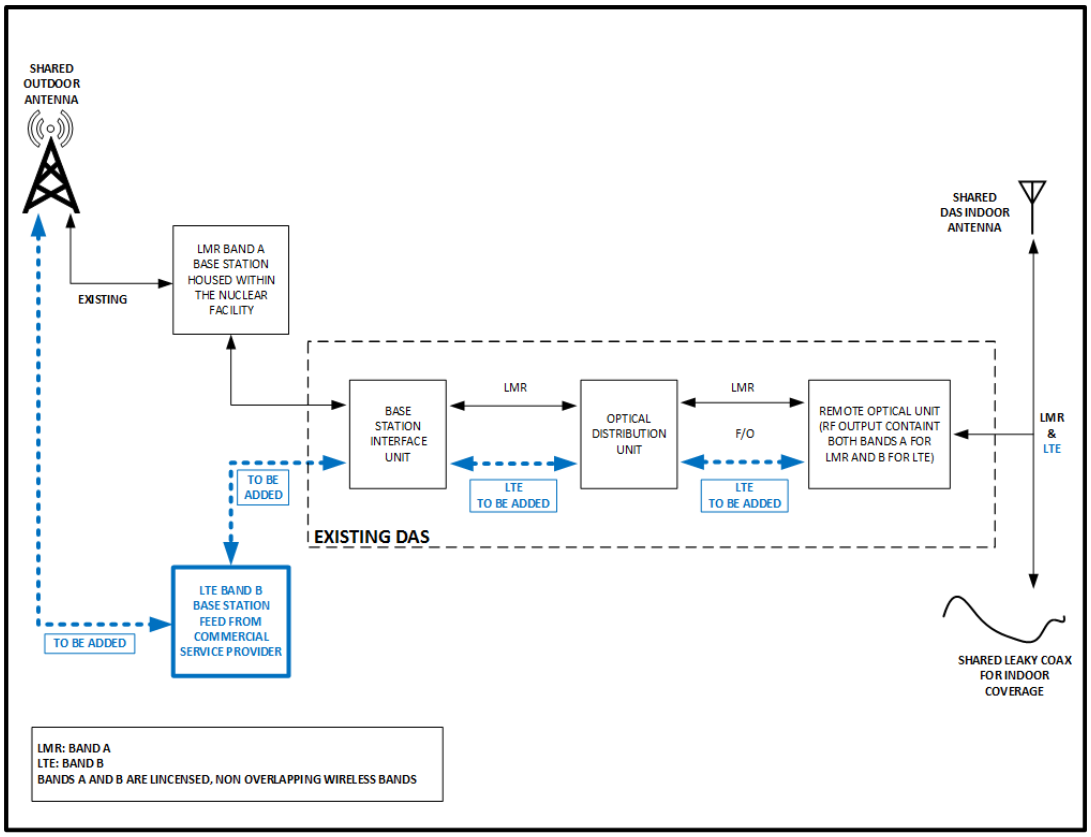

Figure 1. Representative Communication Network Architecture Serving Both LTE and LMR Bands

The LMR communication standard, designated as Project 25 (P25), is a mobile narrowband voice and data communications system with channel widths varying between 12.5 kHz to 25 kHz. The RF coverage for the outdoor plant environment is provided by a conventional antenna system. The RF coverage throughout the indoor of the plant is provided by a combination of leaky coaxial cables and indoor antennas. A DAS interfaces with the LMR base station to carry the communication contents to the various parts of the plant building to be radiated.

The LTE system addition would support a low-security application. LTE is the End to End (E2E) Internet Protocol (IP)-based 4th generation wireless system that is now widely implemented in the United States and elsewhere worldwide. It provides high-speed broadband data services and improved wireless security capabilities as compared to the earlier wireless data networks.

The team detailed the potential architecture for the system and determined which components could interact within the architecture and how that interaction could occur. The main components of a distributed antenna system are the DAS Management System (DMS), Base Station Interface Unit (BSIU), Optical Distribution Unit (ODU), and Remote Optical Units (ROUs) as illustrated in Figure 2.

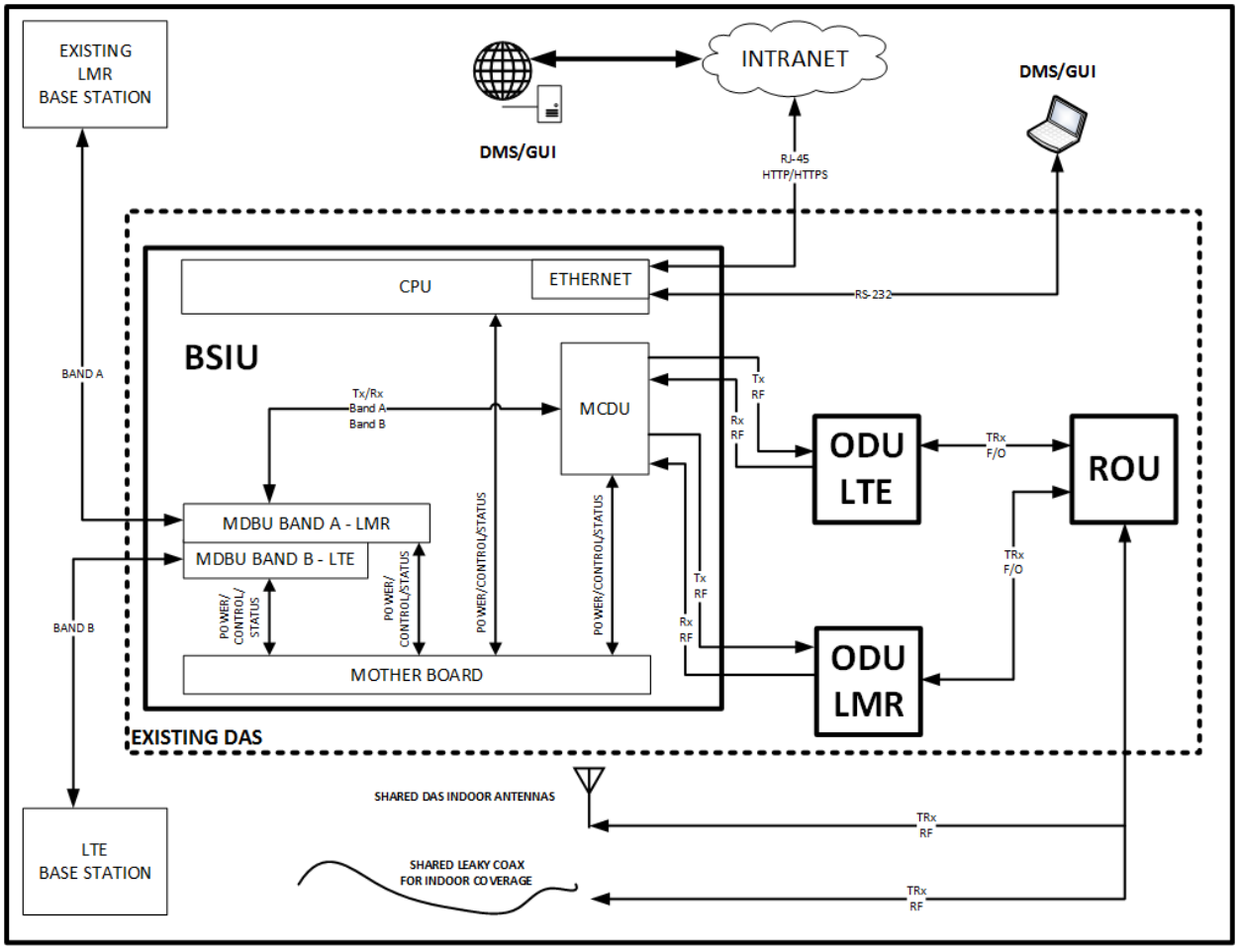

Figure 2. Representative DAS Components.

The DMS is a hardware device that provides a graphic user interface (GUI) to adjust the signal filtering, including the selection of a specific band (low, medium, or high) in each input signal entering the DAS. It synchronizes the signal filters with all of the corresponding ODUs and ROUs. It has additional functionality for upgrading the firmware in one or all devices connected in the DAS. Additionally it can perform a DAS emergency shut off of one or all of the devices (ODUs and ROUs)

connected to the BSIU. The BSIU provides a GUI and receives power, control, and status data flows from each Main Drive BTS Unit (MDBU) and sends them to the Central Processing Unit (CPU) and the Main Combiner Divider Unit (MCDU). The ODUs are responsible for frequency isolation. Once received by the ODU, the signal passes through a 2-way divider/combiner, leaving only the fiber optic outputs of the same optical signal necessary for the ROUs. The ROUs receive optical signals from the ODUs, and transform them from optics to RF before multiplexing and distributing them to the corresponding outputs, such as the leaky coaxial cabling or antennas. Refer to Figure 3 for a generic diagram of a ROU and its components.

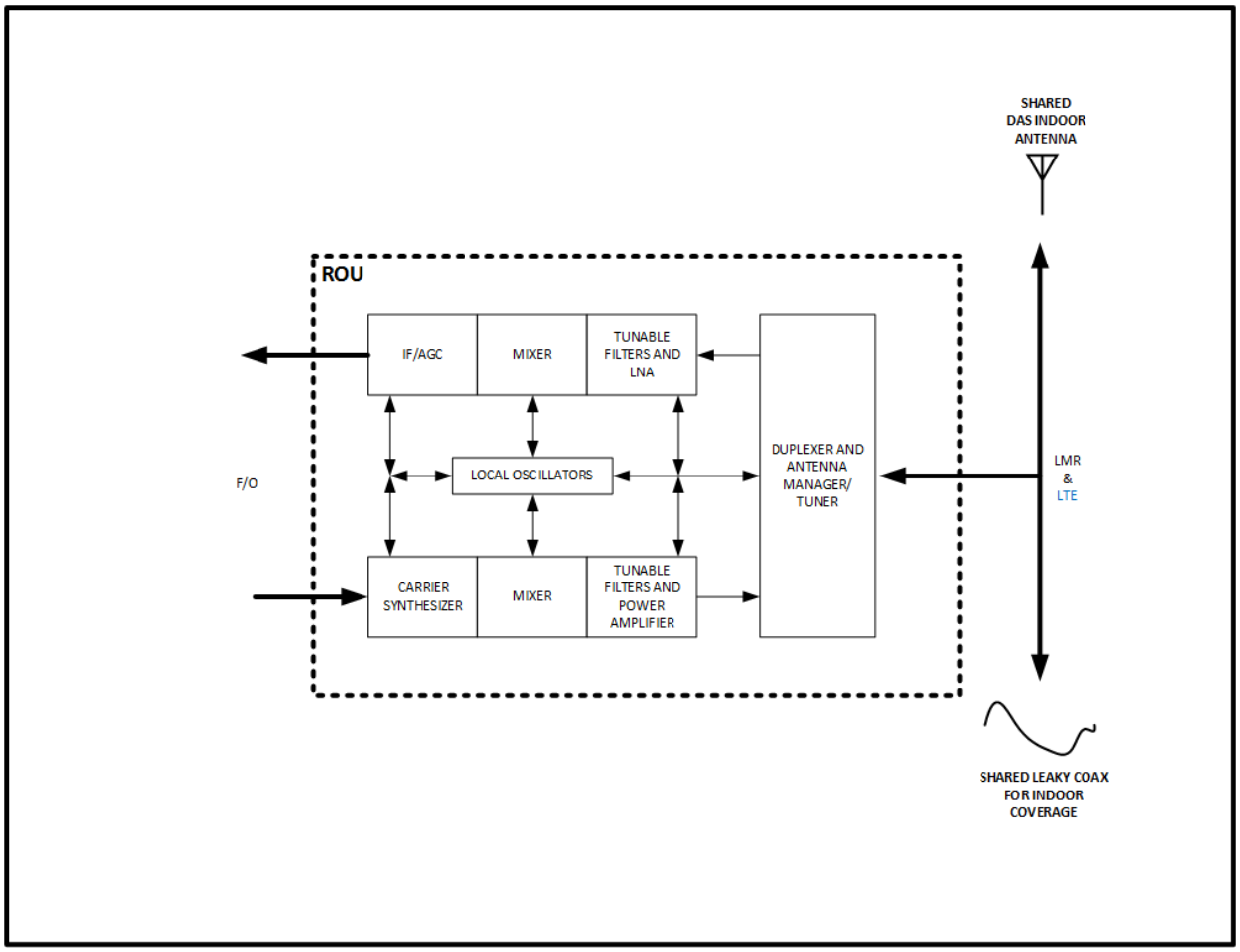

Figure 3. Generic ROU Diagram

4. Security Requirements

The U.S. Code of Federal Regulations 10 CFR 73.54 requires nuclear facilities provide a high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks (Reference 2). The LMR system, in this example, is used for critical voice communications within the nuclear plant and is within scope of this rule. The rule requires that networks used by systems in scope must be isolated from networks used by systems out of scope. The segregation of networks is used as a mitigation for potential cyber-attacks. Adequate controls are in place to provide assurance of the security of the LMR system in its current DAS configuration, without the LTE functionality. Security aspects of the LMR system are well known, documented, and not considered within the scope of this research unless they originate from the LTE system (References 10-12).

Although the data communication served by the proposed LTE addition will greatly facilitate exchange of information, it is not considered within scope of 10 CFR 73.54. LTE security protocols are well known and documented (References 2-8). Specific vulnerabilities and attack scenarios exist which can lead to the disruption of LTE service (References 3-6). The scope of the research team's analysis does not include identifying or analyzing existing LTE vulnerabilities, unless the vulnerabilities can impact the coexisting LMR system.

The addition of LTE functionality to the DAS presents a potential cybersecurity concern and a possible regulatory compliance issue. The cybersecurity concern is that the LTE functionality may provide a cyber-attack pathway to the LMR system. The regulatory concern is that the LTE network and LMR system may not be truly isolated as they share common system components including the DAS, leaky coaxial cabling, and indoor antenna systems.

5. Hypothesis

The EPRI paper posits that because the RF bands used by the two wireless systems (LMR and LTE) are specified to be non-overlapping, and the DAS design is modular, the systems can be considered to be isolated from each other (Reference 1). No extensive analysis has been conducted to determine whether this configuration could allow the LTE system to introduce undesired RF communication signals which could provide a cyber-attack vector for the LMR system.

6. Assumptions

The research team used the following assumptions in their analysis:

1. Although various DAS products are commercially available, we assume that the underlying architecture utilizes typical Software Defined Radio (SDR) design methodology.
2. For the LTE system, the analysis starts from the point where the LTE feed from the commercial service provider, e.g., Verizon Wireless, enters the DAS. The LTE network components (e.g., the base station, called eNodeB) are not included within the scope.
3. The LMR system is licensed and in compliance with 10 CFR 73.54 in its current configuration. Existing known security issues with LMR are not considered within the scope of this research unless they can be targeted from the LTE system.
4. As the LTE system is not within scope of 10 CFR 73.54, and is of low security concern within the proposed architecture, known vulnerabilities for LTE that can be exploited to disrupt the data communication are not considered within the scope of this research effort.

7. Analysis

The team's analysis consisted of detailing the potential architecture for the system, determining which components could interact within the architecture and how that interaction could occur, identifying whether RF could be introduced across the two systems, and determining whether malicious RF artifacts could be introduced from one system into the other.

The shared antenna between the LMR and LTE systems relies on a multiplexer to provide sufficient isolation and attenuation of the respective adjacent channel power. Due to the shared antenna, a communications path exists from the LTE transmit port to the LMR receive path via the multiplexer that provides the necessary attenuation. When operating normally, sufficient frequency separation is maintained between the LMR and LTE systems. It is unlikely that any elevation in the noise floor from the LTE transmit filter skirts that may overlap the LMR band will have a significant impact on performance. If the LTE transmit signal is manipulated to generate spurs or harmonics, however, it is then possible to mix the LTE signal into the LMR band via passive and active components in the RF transmission path. The ability to create suitable mixing products that translate the LTE signal into the LMR band presents a vulnerability to interference from intermodulation products that could possibly degrade or deny communications if the interfering signal is sufficiently powerful.

P25 specifies channel widths between 12.5 kHz to 25 kHz. The 12.5 kHz channel mode is the most robust and critical regarding the ability to maintain communications and therefore will be used as the basis for interference thresholds sufficient to degrade or deny communications. A typical LMR radio operating in a 12.5 kHz channel, utilizing Continuous 4-Level FM (C4FM) or an analog channel with 12dB SINAD, will have a receiver sensitivity of approximately -120dBm. Depending on the system coverage requirements, the output of an LTE DAS power amplifier could range from 1 Watt to 20 Watts (30dBm to 43dBm respectively) or more. Assuming a mid-range power of 5 Watts (37dBm), the span between the LTE output channel power and the LMR receive sensitivity is almost 160dB. The LMR receiver sensitivity level specifies the minimum signal level required for reliable communications and depicts the worst case scenario of when the desired received signal is weakest and thus most vulnerable to interference. Since the radios are mobile, operating near the lower threshold level is a definite possibility. Consideration should be made for the mean signal strength for a given system installation, however.

Representative LMR handsets transmit 1 Watt to 2.5 Watts (30-34dBm). Adjusting the data from the EPRI Crystal River study (Reference 1) to this transmit power level gives an expected received power of -80dBm. Digital modulations are effectively jammed at Eb/No levels of 0dB, whereas the rule-of-thumb for analog modulation is that a SINR less than -10dB is required. Assessing the more robust analog mode, performance degradation begins at interference levels of -80dBm and denial can be expected at -70dBm. Digital channels for this example would become susceptible to degradation at interference levels between -90dBm and -85dBm, depending on coding, with denial occurring at -80dBm. Thus the LTE signal sharing the antenna cable with the LMR system in this example must be attenuated by almost 130dB to ensure reliable communications. This required level of isolation is significant due to the shared medium, and exceeds typical design values for adjacent channel interference (ACI) in Frequency Division Multiple Access (FDMA) communication systems with simultaneous operating channels.

The attenuation requirement to maintain isolation provides a possible vector for both direct noise injection and intermodulation products from the LTE system if components within the RF transmit chain can be manipulated surreptitiously. Methods to facilitate direct noise injection or intermodulation products involve altering LTE subcarrier locations, modulating the waveform itself, and tone insertion. Specific enabling components that are software configurable and/or accessible via remote methods within the RF/optical transmit chain include RF over fiber (RFoF) transducers, digitally controlled oscillators (DCO), automatic gain control (AGC), and variable attenuators.

RFoF components are located in ODUs and ROUs of the DAS. The RFoF blocks convert RF signals to optical signals and vice versa. Since they are the transducers between the RF and optic mediums, direct manipulation of the signals is possible via internal subcomponents – RF Low Noise Amplifiers (LNAs), variable attenuators, and the optical power amplifier. These components are adjustable remotely because the signal parameters must be tuned accordingly for a specific optical link. Additionally, most RFoF units provide test-tone injection modes to test fiber links and provide feedback to set power and attenuation levels. Modulation of the LNA, attenuators, and optical power unit (OPU) provide methods to expand the desired bandwidth occupancy of the LTE signal and create intermodulation products. Saturating the output of the LNA or OPU will result in clipping, which effectively multiplies the intended signal pulse by a square wave that has an infinite response in frequency when expanded as a Fourier series. These spectral harmonics would provide both direct noise injection and mixing products to deliver intermodulation noise back into the LMR receive chain.

Figure 4 shows a spectrally efficient root-raised cosine signal pulse that has an adjacent side-lobe that is 26dB lower than the central lobe as observed in Figure 5. Clipping just the few samples about the peak, as shown in Figure 6, redistributes power from the main lobe to adjacent lobes. The next significant side-lobe for this example is now only 10dB down from the main lobe as plotted in Figure 7. The spectrum outside of the desired LTE band now has prominent power spectral densities and these artifacts can facilitate mixing interference back into the LMR band through passive componentry.

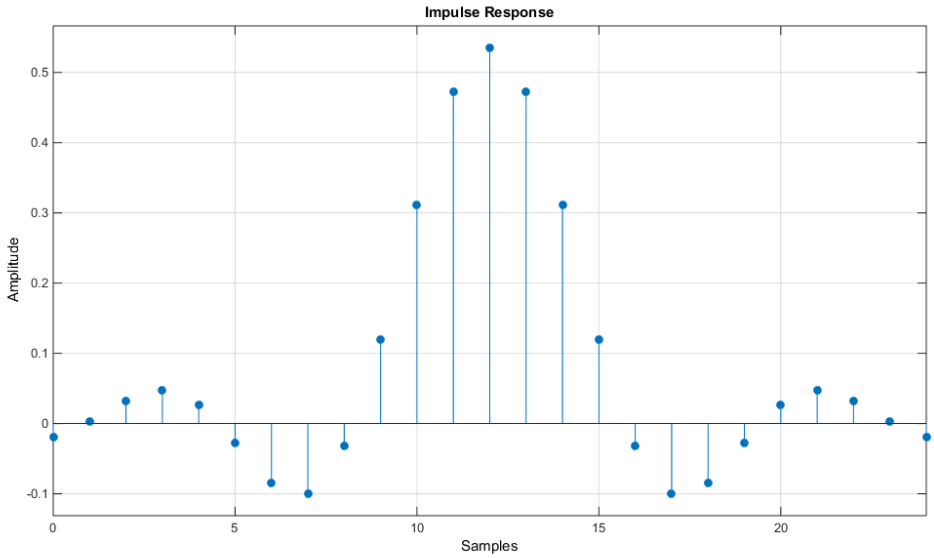

Figure 4. Root-raised Cosine Signal Pulse

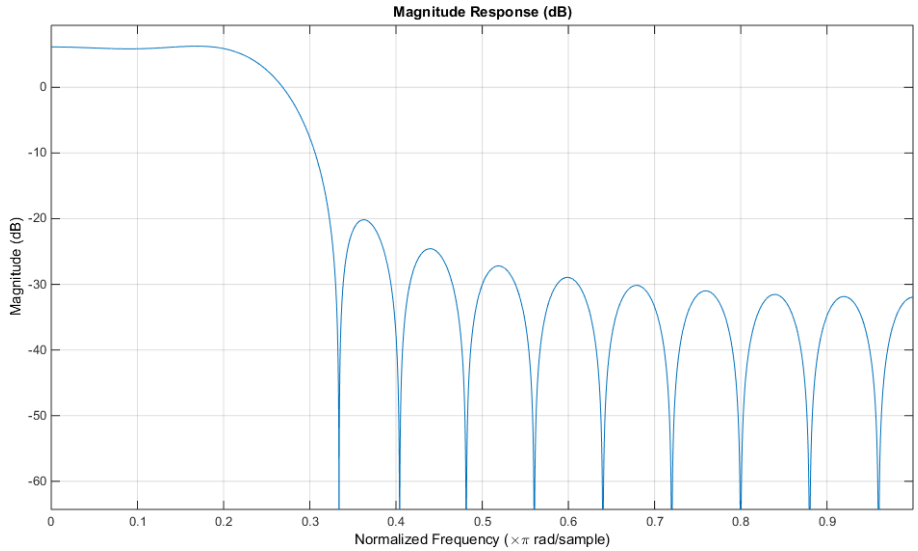

Figure 5. Frequency Response to Root-raised Cosine Signal Pulse

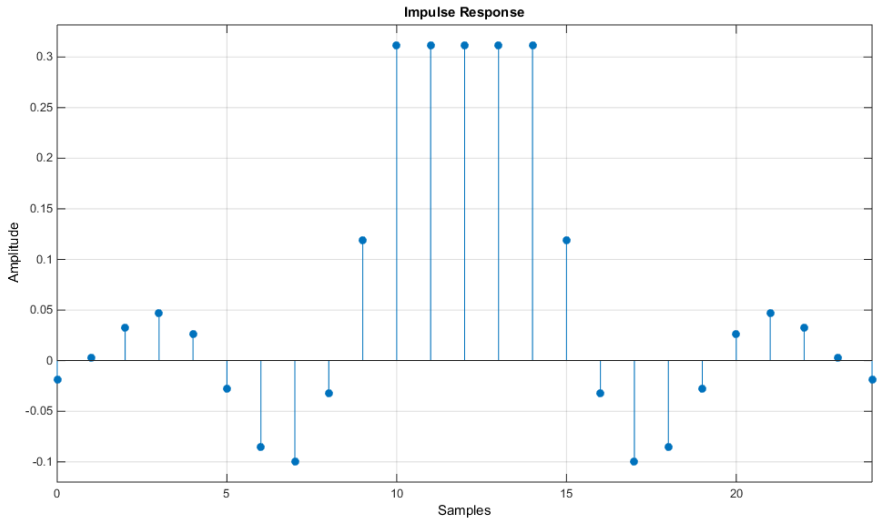

Figure 6. Frequency Response to Root-raised Cosine Signal Pulse

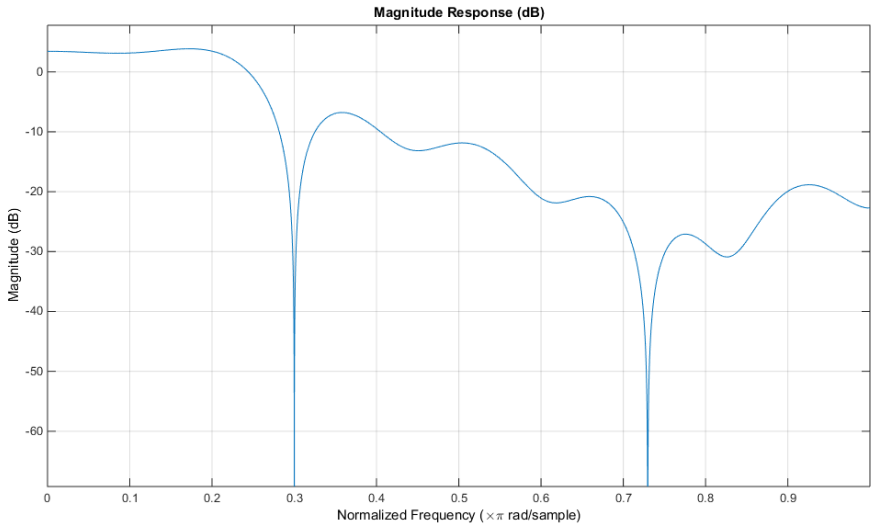

Figure 7. Response to Clipped Root-raised Cosine Signal Pulse

The DCOs within the ROUs can be manipulated by adjusting the register value which sets the frequency for the RF upconversion. Dithering, chirping, or hopping frequency in discrete increments will alter the spectral characteristics of the desired LTE waveform. This will produce out-of-band components, similar to manipulating the RFoF block, which can possibly be mixed into an LMR channel.

The AGC circuit, located within the BSIU, conditions the downlink LTE feed signal prior to distribution from the DAS. The AGC contains multiple settings effecting the output that are set from configuration bits, i.e., target output level, signal frame time, hold time, decay rate, and maximum gain. Adjusting the target output to values at or near the maximum gain level of the AGC removes any margin the AGC may need to compensate for unexpectedly strong signals. Additionally, if the signal time frame and hold time settings are manipulated to exceed the channel's coherence time, the AGC will not be able to appropriately respond to signal power fluctuations present in any typical channel. This will result in

AGC output saturation which can produce clipping and harmonics with significant power spectra since the AGC is an active component.

Variable attenuators condition the signal in concert with the AGC to ensure the input signal to the ROU will not saturate the output. These electronically controlled devices have typical response times of only 100 nanoseconds, making them ideal amplitude modulators for the output signal. Inverting or disabling the control response for the variable attenuators will allow signals to saturate the ROU's power amplifier creating signal distortion and harmonics from the most impactful active component in the transmitter chain.

The team's analysis identified the potential to introduce RF across the two systems, violating the assumption of isolation. The team further determined a possibility exists for the two systems to introduce potentially malicious RF artifacts into one another.

8. Findings

Prior to this project, no extensive analysis had been conducted to determine whether cyber manipulation could enable RF signals from one system to influence another while sharing a DAS, leaky coaxial cable, and antennas. These findings are believed to be plausible as a cyber manipulation vector to influence operations of another system.

The downlink signal conditioning path provides several components that can produce output signal distortion in adjacent bands either directly or through intermodulation products mixed by active and passive componentry when manipulated, misconfigured, or disabled. Specifically, the AGC, variable attenuators, DCO, and RFoF components all provide methods to modulate, distort the signal, or inject tones through digital parameter manipulation.

Modulation of the LNA, attenuators, and OPU provide methods to expand the desired bandwidth occupancy of the LTE signal and create harmonics and intermodulation products. These spectral harmonics would provide both direct noise injection and mixing products to deliver intermodulation noise back into the LMR receiver chain; this can be accomplished remotely. Misconfiguring the AGC and control response of the variable attenuators limits the amplitude response of the transmission chain to normal signal fading received at the DAS input. This prevents large signal amplitude swings from equalizing properly, thereby creating clipped signals and saturating amplifier outputs. Disabling the variable attenuators at the ROU power amplifier input removes the transmitter's ability to prevent saturation and subsequent harmonic distortion. Generating harmonics at the power amplifier's output is particularly insidious as this is the juncture in the transmission chain at which interfering signals have the opportunity to acquire the most signal power. Manipulation of the DCO allows specific carriers or tone creation that can target the calculated intermodulation products needed to mix interference into the desired band. Additionally, dithering, chirping, or hopping frequency in discrete increments will alter the spectral characteristics of the desired LTE waveform. This will produce out-of-band components, similar to manipulating the RFoF block, which then can possibly be mixed into an LMR channel.

The requirement of modern radio systems to provide the ability to remotely configure and maintain system performance are inherent vectors to manipulate parameters that effect radio operation and output spectral characteristics. Electronically configurable components inherently present in typical software-defined radio that could provide methods to manipulate communications on the targeted adjacent LMR channel have been identified and analyzed.

9. Future Research

This research was limited to an analysis of two wireless systems sharing a DAS, antennas, and leaky coaxial cabling, and experimentation on specific systems was not performed. Additional research remains to be conducted on this topic, including 1) experimentally validating specific vulnerabilities for this configuration can be exploited by cyber manipulation, 2) designing controls to mitigate those

vulnerabilities, and 3) developing intrusive tests to confirm that the control mechanisms function properly. Additional research could be performed to develop frequency separation techniques to mitigate the potential for malicious influence.

10. Conclusions

This research effort set out to investigate the assumption of isolation between two wireless systems, specified to be non-overlapping, when they share a DAS, leaky coaxial cabling, and indoor antenna system. The example systems were a low-security system using LTE wireless data services and a high-security system using LMR wireless voice service. This paper investigated how the security of the LMR voice network may be impacted by sharing its resources with the LTE data network. The research team performed an analysis of the LTE input points, output points, and management components within the DAS. Although the two networks were shown to operate correctly under normal operating conditions, the analysis identified areas where the LTE system could introduce undesired RF communication signals for the LMR system.

11. References

1. EPRI, 2017, *Use of LTE Cellular Network and Distributed Antenna Systems to Improve Connectivity and Increase Data Transfer*. Electric Power Research Institute, Report No.: 3002009128, March 2017.
2. 10 CFR 73.54, 2015, *Protection of digital computer and communication systems and networks*, Code of Federal Regulations, Nuclear Regulatory Commission, December 2015.
3. Dan Forsberg et al.t, *ENHANCING SECURITY AND PRIVACY IN 3GPP E-UTRAN RADIO INTERFACE*, The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Athens, Greece, September 2007.
4. Altaf Shaik et al., *Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems*,, Network and Distributed System Security Symposium, San Diego, California, January 2016.
5. Roger Piqueras Jover, *LTE security, protocol exploits, and location tracking experimentation with low cost software radio*,, Bloomberg LP, New York, NY, July 2016
6. Roger Piqueras Jover, *Enhancing the security of LTE networks against jamming attacks*, EURASIP Journal of Information Security, April 2014
7. Jeffrey Cichonski et al., *Guide to LTE Security*, NIST Special Publication 800-187
8. Dan Forsberg et al., *LTE Security*, John Wiley & Sons Ltd, ISBN 9780470661031, 2010
9. Yulong Zhou et al., *A Survey on Wireless Security: Technical Challenges, recent Advances, and Future Trends*, Proceedings of the IEEE, Volume 104, Number 9, September 2016.
10. Sandy Clark, Perry Metzger, Zachary Wasserman, Kevin Xu, and Matthew A. Blaze. *Security Weaknesses in the APCO Project 25 Two-Way Radio System*, University of Pennsylvania Department of Computer and Information Science Technical Report No. MS-CIS-10-34, November 2010.
11. Matt Blaze, with Sandy Clark, Travis Goodspeed, Perry Metzger, Zach Wasserman and Kevin Xu. *Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System*, SEC'11 Proceedings of the 20th USENIX conference on Security, San Francisco, CA, 2011.
12. Glass, Steve; Vallipuram, Muthukkumarasamy; Portmann, Marius; Robert, Matthew. *Insecurity in Public-Safety Communications: APCO Project 25*. 7th International ICST Conference on Security and Privacy in Communication Networks, London, September 2011.