NISTIR 8195

Requirements for Spectrum Monitoring in Industrial Environments

Murat Aksu
Richard Candell

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8195

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8195

Requirements for Spectrum Monitoring in Industrial Environments

Murat Aksu
Richard Candell
Intelligent Systems Division
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8195

November 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Abstract

Spectrum monitoring serves as the eyes and ears of the spectrum management process and helps spectrum managers to plan and use frequencies, avoid incompatible usage, and identify sources of harmful interference. The key objective for this research at the National Institute of Standards and Technology (NIST) is to develop a prototype for spectral analysis of both licensed and unlicensed radio frequency (RF) bands, allowing the monitoring of the industrial environment and the access of that information in a simple way for use at industrial facilities with noisy environments and real-time performance requirements, including factories, warehouse and discrete manufacturing, assembly, robotics, oil and gas refineries, and water and wastewater treatment plants. This paper provides the specification of industry requirements of spectrum monitoring systems in industrial facilities, so that NIST research will meet these needs.

Keywords: Spectrum Monitoring; Spectrum Management; Wireless Networking; Industrial Control

Disclaimer: Commercial equipment and materials are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 PURPOSE AND SCOPE OF THIS DOCUMENT

The purpose of this document, whose scope is the specification of industry requirements of spectrum monitoring systems in industrial facilities, is to serve as guidance for spectrum monitoring in those harsh industrial environments.

1.2 AUDIENCE

This document is directed toward manufacturing or processing facilities that use wireless sensing, supervisory control, and feedback control where unexpected improper operation may create a safety risk or cause economic loss. The intended audience can be varied, including the following:

- System integrators who design or implement a spectrum monitoring system
- Plant operators who are trying to understand implications as they apply a spectrum monitoring system to help mitigate the impacts to business operations
- Device manufacturers that are developing products which will be deployed as part of a spectrum monitoring system
- Information Technology (IT) and Operational Technology (OT) security officers interested in monitoring electromagnetic spectrum for intrusions and anomalies

1.3 DOCUMENT STRUCTURE

The remainder of this document is divided into the following major sections:

- Section 2 provides the importance of the spectrum monitoring for planning channel/band usage and identification of harmful interference.
- Section 3 provides current state of practice for industrial spectrum monitoring systems.
- Section 4 provides a reference architecture for Industrial Control Systems.
- Section 5 addresses industrial case studies in which spectrum monitoring would have been crucial to apply to help mitigate the impacts.
- Section 6 explores functional requirements for the spectrum monitoring system.
- Section 7 provides conclusions.

2 PURPOSE OF SPECTRUM MONITORING

In today's industrial environment, the use of wireless devices and systems is proliferating at a rate beyond the user's ability to understand, monitor, and control effectively. Many systems operate in unregulated frequency bands and have never been subjected to testing to assess how their performance might be affected by other systems that share the spectrum. Modern industrial facilities can have hundreds or even thousands of wireless devices. It is no longer practical or cost effective to attempt to troubleshoot issues with wireless systems by having someone “walk around” with a portable spectrum analyzer and a hand held directional antenna trying to determine the source of an interfering signal. In today’s complex and dynamic environment, this goes beyond even the concept of a needle in a haystack, where now there are many different types of needles among many different types of hay. Manual techniques can only be effective if the signal can readily be distinguished from the overall radio frequency (RF) environment. In addition, this method requires a skilled operator. It is clear that yesterday's spectrum monitoring methods are not up to the task of today's spectrum management challenges, which requires a different paradigm.

This new more proactive paradigm makes the distinction between spectrum monitoring and active spectrum management. Monitoring is an open loop process where tools and methods are used to determine what is there at any given instant in time, to make sense of it, and possibly undertake further investigation such as the previously described manual signal hunt. Management, by contrast, is an active process where a desired state, in this case use of the spectrum, is known and a closed loop system is in place to compare the current state with the desired state and then take specific focused action to return the system to the desired state. As Prof. Peter Drucker once said [1], one of the fundamental tenets of management is that “You cannot manage what you do not measure.” This is precisely the challenge facing spectrum use and problem resolution today. A system is needed that provides automated tools to compare the spectrum with what is expected, to identify signals that should not be there and thus could be interference sources, to verify that they are in fact interference sources so limited resources are not spent locating emitters that in fact are not causing problems, and then to locate true sources of interference so they can be mitigated. The end goal should be to have a system that can provide autonomous RF situational awareness for a manufacturing facility on a 24/7/365 basis with minimal operator intervention with the capability to quickly react to abnormal situations and to support prompt resolution.

3 CURRENT STATE OF PRACTICE

After consulting with a variety of spectrum monitoring solutions providers in the industry, we note that industrial control sites typically operate in the unregulated industrial, scientific, and medical (ISM) band between 902 MHz and 928 MHz. Spectrum monitoring today focuses mainly in this range. While the devices operate at low power levels, periodically a rogue emitter might interfere with the operation of these devices and cause a disruption in the production process or vital communications. The emitter might last from a few seconds to up to 30 minutes. The interference events might increase from once or twice a month, to a few times per week. Sometimes the interference might occur during normal operations, and other times, it might happen off hours. Sitewise, there might be building structures and communication towers.

An industrial site might have two issues: The first is that its own operations might be disrupted by these events. The second is the need to confirm or challenge the source of the interference. Operationwise, an industrial control site should have an IT staff and a NOC (Network Operations Center) to monitor industrial control stations.

From a requirements perspective, site personnel might be mainly interested in being notified and alarmed when a signal in the 902 MHz – 928 MHz breaks a certain power threshold. When this event occurs, personnel might want to capture the event, including the direction of the interferer, and be able to analyze the data. A main control station might be located at the NOC, and this is where personnel might want to be notified. If the event happens off hours, personnel might want to view the event the next business day and their desire might be to have minimal operator interaction, beyond "setting and forgetting" the main system. A system would run continuously 24/7 and only be taken down for maintenance from time to time. Given the size of an industrial site, personnel might need to operate a portable unit to further isolate the source.

Given the power and duration of the signal, and the general desire to locate the source, site personnel might be well suited to start with a direction finding (DF) antenna running with a spectrum monitoring software. A system would run 24/7 and generate a notification and alarm during an event. Once the system is set to run, there is little operator dependence required until an event occurs.

Considering the number of structures, commercial traffic, and continuous construction, site personnel would also benefit from having at least one portable receiver to further isolate the emitter. Practically speaking, the operator would get a line of bearing (LOB) and can deploy a portable receiver during an event providing that the signal is active.

Also, it is worthy of mentioning some of the examples of the application of advanced monitoring techniques, such as Global System for Mobile communication (GSM) base station geolocation, correlation application in satellite interference finding, and spatial spectrum based beam-forming in high frequency (HF) / very high frequency (VHF) monitoring, which can be found in [2].

4 INDUSTRIAL CASE STUDIES

Modern industrial facilities increasingly rely on wireless devices such as production and material handling equipment, inventory tracking, and handheld devices used by operators and managers. Some of these large facilities can have thousands of wireless RF devices all operating simultaneously. Unfortunately, additional personal devices that share the same spectrum might often be brought into these facilities by employees, vendors, and maintenance workers which would cause interference, disrupting daily operations and resulting in downtime and hazardous situations in some cases. In this section, we will give some industrial case studies to show how much time and effort would have been saved if there were a spectrum monitoring system deployed in these facilities.

The following subsections are based on personal interviews of actual events. Technical details were not conveyed during the interviews. The bottom line was that the interference was strong enough to overwhelm factory instrumentation.

4.1 Defense Manufacturer Incident

At a large commercial manufacturing facility with over 3,000 wireless devices in use for industrial control, material handling, and a wide range of manufacturing support purposes, some equipment suddenly failed to function properly. This disrupted on-going manufacturing operations, creating potential for safety hazards and causing a significant loss of productivity. This incident occurred over several days, and in the absence of a spectrum monitoring capability, all that could initially be determined was that the equipment was malfunctioning intermittently. Staff spent several days troubleshooting the equipment, mistakenly thinking that it was the source of the problem, and it took time to determine that the source of the problem was interference with the wireless link rather than an antenna or modem problem. At that point, the staff called in their RF team, who did a scan of the spectrum using a handheld spectrum analyzer. This was challenging since the interference was not continuous, but at some point, the team saw an unexpected signal occur. Tuning to it, they were able to hear two people talking to each other, and wrote down their names. They then went around the facility individually asking personnel about the identities of the two people. Eventually they determined that a contractor did indeed have two people with those names working on a crane. These contractors, innocently, but without coordination, were using ISM band hand-held radios which interfered with wireless production support equipment using the same ISM band.

The advantage of a permanent spectrum monitoring system is that it can "learn" the normal RF environment and look for anomalies. In this situation, if the staff had a simple monitoring capability, they could have received an alarm the first time the workers used their radios in the building. With a few RF sensor nodes inside and outside, they could have instantly verified if the signal was coming from inside the building or from somewhere outside but presumably near the building. With a distributed network of RF sensor nodes, they could have had an immediate indication of at least approximately where the transmission was coming from, all from the first transmission.

4.2 An Oil & Gas Refinery Incident

One oil and gas refinery operator situated on the Gulf of Mexico made plans to build out its wireless instrumentation infrastructure at the request of their control engineering staff. At the time of their plan to deploy wireless devices, it was not possible to obtain exact numbers and types of wireless devices. The operator considered three wireless protocols: Wi-Fi, WirelessHART, and ISA 100.11a. Wi-Fi is a popular consumer protocol with high bandwidth, but not designed specifically for industrial use. WirelessHART and ISA 100.11a were intended for industrial applications, supporting deterministic real-time communication but at the lower bandwidths typical of sensing and control. Based on cost and performance considerations, the operator selected WirelessHART. They estimated within their first year that dozens of sensing devices would be deployed within the buildings housing their distillation furnaces; however, they did have a sense of the benefit that wireless sensing could bring to their operation and desired to deploy more over time to their steam traps, pipes, and tanks. In addition to process monitoring, they also had plans to use wireless as either a primary or backup solution for safety tethers used when staff were performing maintenance within confined spaces.

In order to make the wireless deployment successful, the refinery operators understood that monitoring their spectrum would be an important part of their wireless program. They desired to have a way of monitoring the spectrum for detecting and geo-locating spectrum anomalies inside and outside of the RF operating band. They also desired to have the ability to project future spectrum usage based on historical usage patterns, thereby making deployment of access points more proactive. This is often identified as wireless “situational awareness.” After meetings with the operator, they requested that NIST develop guidance that industry could use to select and deploy a wireless situational awareness application within their factories.

This refinery operator also had a situation in which a local truck driver wary of wireless tracking devices installed a jamming device in the cab of his vehicle to obstruct any tracking devices installed by the owner of the refinery. The jamming device was a small module that fit into the automobile power socket, but was powerful enough to disrupt factory communications every time he drove past the refinery. After weeks of guesswork and spectrum tracking along the perimeter of the refinery, it was determined that the driver was responsible and appropriate action was taken. A lessons-learned analysis showed that an active listening solution with geolocation capabilities could have pin-pointed the emitter early making the disruption easier to correct.

4.3 Wireless Crane Tele-Operation Incident

A manufacturer of commercial passenger aircraft had an incident where the operation of a heavy-lift overhead crane failed to operate due to a disruption in communication between the crane and the wireless remote controller. The communication link between the crane and the remote was governed by a frequency shift keying (FSK) - based 902 MHz to 928 MHz transceiver. The operator hypothesized that the wireless link was compromised by using a simpler spectrum analyzer. It was assumed that the emitter was within the factory, based on the signal strength measured by the spectrum analyzer. After many hours of searching for a rogue emitter using word-of-mouth and rudimentary emitter geolocation, it was found that two factory employees purchased citizens band (CB) radios so that they could more easily communicate and perform their respective jobs better.

While this self-initiative was commendable, this action by the employees caused an operation outage that could have been prevented through better education about wireless operation. Furthermore, the outage could have occurred while the crane was in full operation increasing the likelihood of injury to people or property. A distributed spectrum monitoring system could have detected the situation, identified the location of the emitters, and allowed operation to resume faster. Moreover, if the spectrum monitoring system had been integrated with the crane operation system, it could have prevented operation through a safety interconnect or somehow allowed the wireless remote to adapt by tuning to a different center frequency. Finally, an active spectrum monitoring system could have notified the appropriate personnel of a rogue emitter long before crane operation had been scheduled.

5 FUNCTIONAL REQUIREMENTS FOR SPECTRUM MONITORING

Increasing reliance on wireless devices which must share the limited RF spectrum will create more opportunities for interference that will disrupt operations and may create safety hazards at industrial facilities. This interference may be caused by unauthorized transmitters or authorized emissions causing unintended outcomes such as harmonics. It is also crucial to understand the current usage of the spectrum as a baseline for future planning. This can be determined from existing data of frequency usage across the entire radio spectrum. Industrial facilities need effective and simple means to monitor the RF spectrum inside or outside of their facilities so that they can proactively identify interference situations and support prompt resolution.

There is no single universal set of specifications for spectrum monitoring that will encompass all types of industrial environments since their RF footprint is different. In this section, we will provide some of the important functional requirements which are generic enough to apply broadly to these industrial facilities.

A generic spectrum monitoring system architecture is given in Figure 1. A spectrum monitoring system should include two main components: Real-time analytics and offline analytics. There should be a threshold value set for monitoring sensors to listen to. During real-time analytics, if aggregators see a signal which is important, they should send that to the aggregation server right away which is an unscheduled event. If the aggregation server decides that this information meets criteria based on the application/script running, it should notify personnel by setting off an alarm, sending an e-mail or short message service (SMS) message. The aggregation server should periodically poll trace data and metrics data, and store that in the metrics database for offline analytics. Example metrics should provide the user with situational awareness.

Also, there are data that should potentially go to a cloud application which makes the data available to mobile applications.

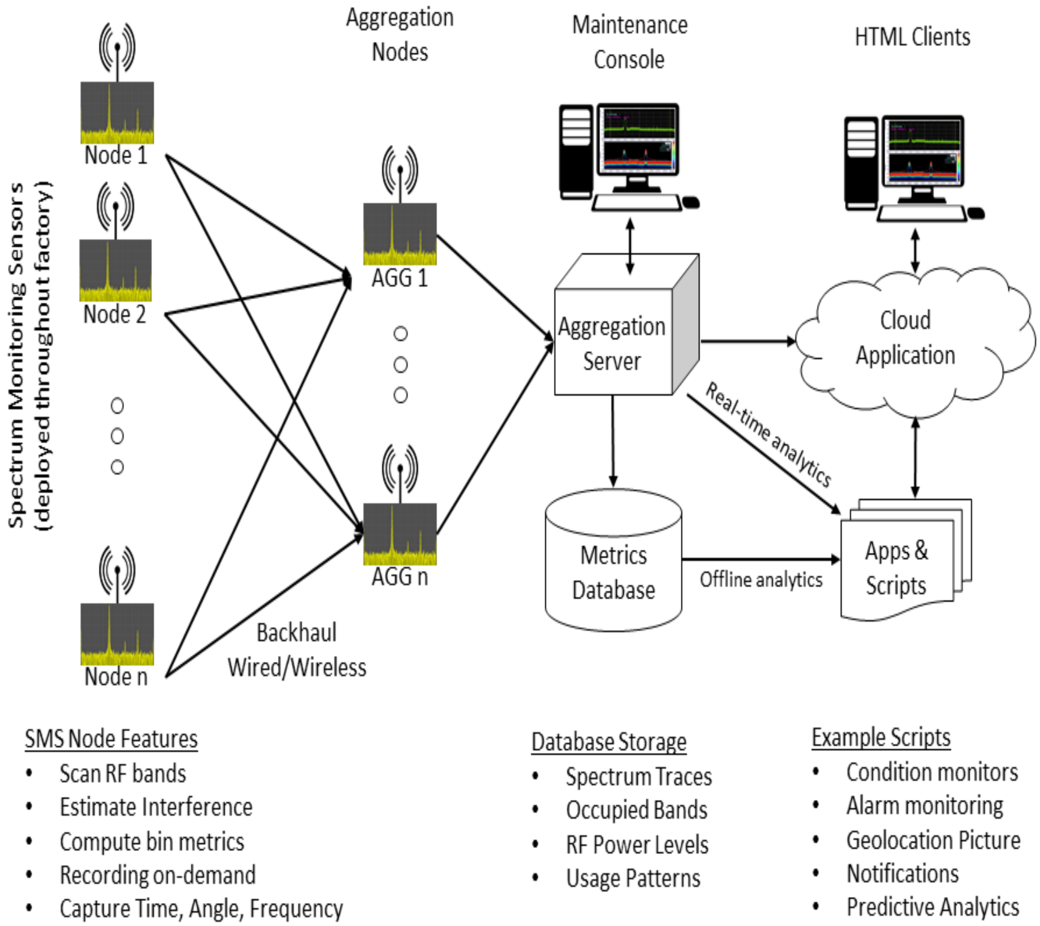

Figure 1. Generic Spectrum Monitoring System Architecture

A spectrum monitoring system at industrial facilities should include the following key features:

Table 1. Functional Requirements for an Industrial Spectrum Monitoring System

Functional Requirement	Description
Continuous Spectrum Monitoring	Continuous spectrum monitoring should be preset by the operator to run for a specified period of time. Many operators requiring continuous spectrum monitoring will run the system 24/7 and want to be alarmed and notified if a disruption occurs.
RF Spectrum Coverage	RF spectrum coverage for spectrum monitoring including direction finding should be typically 20 MHz – 6 GHz. There are many technical and environment considerations when defining the RF spectrum coverage for spectrum monitoring system.
Close Proximity Spectrum Monitoring	Close proximity spectrum monitoring relates to installations near powerful transmitters, or cable length from receiver to antenna (line loss).
Rogue Emitter Geolocation	Rogue emitter geolocation is provided by taking more than one line of bearing (LOB – single measurement on an emitter) to form an intersection on a target and often displayed on a map. Finding rogue emitters can involve either (or both) stationary or moving spectrum monitoring assets depending on the operating environment.
Distributed Spectrum Sensing Architecture	RF spectrum sensor units should be working together in a coordinated way to detect and confirm anomalies.
User Interface	User interface should be flexible based on use case and operator skill level.
Notifications and Alarms	Spectrum monitoring system should provide a broad base of options to be notified and/or alarmed during an RF event.
Historical Database	Database for spectrum monitoring system should support various use models that involve local, remote, import and export, and query analysis options.
Industrial Control System Integration	Integration of control systems with spectrum monitoring system such that the control system can adapt to the situational awareness of the RF spectrum.

5.1 Continuous Spectrum Monitoring

Continuous spectrum monitoring, as the name implies, is preset by the operator to run for a specified period of time. Depending on the use case, an operator may want the system to run on certain days of the week, or perhaps during a specific event. Many operators requiring continuous spectrum monitoring will run the system 24/7 and want to be alarmed and notified if a disruption occurs.

When planning a continuous spectrum monitoring solution such as the 24/7 model, automated and unattended capability should be generally favored over operator dependent activities unless the industrial facility policy requires that the system be attended. At a practical level, a spectrum monitoring system should provide the operator with flexibility to operate the system in an unattended and/or remote networked accessed mode, or an attended locally controlled mode.

5.2 RF Spectrum Coverage

The RF spectrum presented in context to industrial spectrum monitoring should be generally considered 20 MHz to 6 GHz due to the fact that these high demand bands are particularly useful for broadband applications. When examining a spectrum monitoring system, the frequency range of interest should be specified. In general, the tighter the frequency range, the more refined the antenna design will be. Also, understanding the target signal environment is essential. RF interference and disruption are usually derived from: communication transmissions, collocated transmitters, bi-directional amplifiers (BDAs), broadcasters, intentional interference such as jammers, spurious unintended emissions, or a change in environment such as new construction, to name many.

Considering performance areas, such as sensitivity, accuracy, scan speed, signal duration, operating modes, coverage area, site suitability, operator skills sets, and other factors, should be captured in the planning phase as well. In an industrial setting, an operator can anticipate operating in a crowded RF space along with having to deal with RF reflections/refractions. Covering a desired frequency in an urban/RF crowded environment as compared to an open rural area will drive different solutions. This includes how the technology will be deployed and the level of expertise needed to operate the spectrum monitoring assets.

Additionally, certain hardware properties are needed for continuous spectrum monitoring. As previously mentioned, typical spectrum monitoring RF sensor units can usually tune a wide range of carrier frequencies, such as from 20 MHz to 6 GHz. Instantaneous bandwidth that is supported by such units is usually less than the carrier frequency range, and may be up to 100 MHz. However, these parameters are not valid for continuous spectrum monitoring. This type of monitoring is applied in order to observe a determined frequency band without changing carrier frequency frequently. Because of the limited number of carrier frequency changes, the supported range of instantaneous bandwidth should be higher and desired frequency band should be monitored without any division.

Beyond these parameters, there are some other parameters which need to be considered. Spurious-free dynamic range (SFDR) of the related hardware should be high in order to obtain a qualified monitoring performance and detect desired signals properly. Noise figure of the hardware should also be considered for proper performance. Typical commercial spectrum monitoring systems use values of minimum 60 dB for SFDR and less than 10 dB for noise figure.

Specifications of these parameters should be evaluated with the scope of the particular industrial application and financial resources. Moreover, features of the monitoring units included in the market should be evaluated and related parameters should be adjusted accordingly.

5.3 Close Proximity Spectrum Monitoring

Close proximity spectrum monitoring is a term that typically refers to operating close to a powerful transmitter without either overdriving the receiver or destroying the antenna and/or receiver or coupling the receiver close to the antenna to reduce line loss.

When operating a spectrum monitoring system in close proximity to a powerful transmitter such as a radio or television (TV) broadcast station, the monitoring system is susceptible to being overdriven or damaged/destroyed. To mitigate such environments, RF spectrum monitoring sensor units should include pre-selection (filtering banks) and automatic gain control (AGC), which is the hallmark when choosing a spectrum monitoring system, to block-out the unwanted transmission by subdividing the input frequency range into subranges via switches and filters to reduce the signal sum load on the input of the sensor unit’s first mixer to allow monitoring of widely different signals. The sensor unit’s AGC subsystem can sense changes in the RF environment to secure the integrity of the signal being monitored. Since the filter banks weaken the power of the strong signal in the band of interest and AGC is being utilized, this will allow for the weaker signals to be monitored within a pre-selected band.

5.4 Rogue Emitter Geolocation

As society becomes increasingly dependent on wireless technologies, the opportunity for disruption from rogue sources also increases. When considering an industrial environment, any form of wireless dependency disruption can result in lost productivity and perhaps create a safety issue.

An operator may be able to resolve an interferer using a portable spectrum analyzer by manually taking measurements with one or multiple devices, eventually resulting in a triangulation which will be discussed in the next paragraphs. However, if an RF emitter/interferer is intermittent, or is located in a harsh RF environment, the instrument may quickly become overdriven and not useful. In the case of a highly reflective environment, it may never see the signal or be chasing an RF reflection.

In practical terms, geolocation (aka "fix") is provided by taking more than one line of bearing (LOB – single measurement on an emitter) to form an intersection on a target and is often displayed on a map. The optimal fix is where two lines intersect at a right angle. If multiple sites are networked together, then two or more systems are required to see the signal at the same time and capture the event.

Finding a rogue emitter is case-by-case specific and can involve both stationary and mobile spectrum monitoring tools. For example, if an operator is operating in an urban environment and has two fixed stations, geolocation is difficult if the target is stationary and behind a building/in a location where there is not a line-of-sight (LOS). However, if the operator has mobile assets, they can be positioned in an area where an emitter can be seen. Moreover, if an emitter is moving, then the fixed stations have a likely better chance of seeing the signal as the target tracks.

A qualified signal processing methodology should be implemented in order to locate the source of a rogue emitter. Security of industrial radio networks is becoming more important, because such networks are crucial for effective performance of an industrial facility and can be attacked easily by tracking data exchange between the monitoring system and field devices. Furthermore, such attacks are difficult to detect and efficiency of the network can be downgraded easily. In order to manage these security threats and locate rogue emitters, RF spectrum monitoring sensor units should have effective signal processing algorithms. For detection of an emitter's location, triangulation and trilateration methods can be utilized to estimate the position of the receiver given the angle between each transmitter and the main axis of the receiver's antenna and the distances from the receiver to each of the transmitters, respectively.

5.5 Distributed Spectrum Sensing

It is vital to maintain situational awareness of the spectrum environment to ensure full-spectrum superiority. The spectrum monitoring system operating on the basis of distributed RF spectrum sensor units should provide imperative data for frequency situational awareness by working together in a coordinated way to detect and confirm anomalies in the spectrum, measure the complete range of frequencies, and capture weak signals.

Since spectrum usage can differ by both time and location within an area, more measurements would be needed from different locations by deploying a network of monitoring sensor units which can autonomously execute their tasks to provide statistically valid data. These remotely deployed sensor units should be connected over a transmission control protocol/internet protocol (TCP/IP) network, including cable, fiber, and cellular. TCP should be used for administrative tasks, such as configuration and monitoring of individual sensor units, that require reliability and compatibility.

A spectrum monitoring system might produce up to a few gigabyte (GB) of data per hour, and thus effective data compression should be applied to curtail the backhaul requirements. The compressed data should be stored locally in the sensor unit and transmitted to the central control server in a form permitting database searches by time, location, and frequency. In the event of interruption of transmission, the data should be retrieved from the remote sensor unit allowing to create a database with true spectrum usage data.

5.6 User Interface

The spectrum monitoring system should provide an easy-to-use graphical user interface (GUI) with the ability to simultaneously display the spectrum use and/or segments of the spectrum in a number of ways. Generally, the industrial operators of spectrum monitoring systems can either feed received data into their own system software, or utilize the device manufacturer provided interface. The individual RF sensor units should be able to be accessed by different spectrum monitoring centers to support different types of monitoring and analysis functions. The user interface should be designed to present a variety of formats depending on use case and operator experience. For instance, some operators may want to see a LOB or FIX on a map display, while other operators may want to see the spectral environment. Depending on the system configuration and options, the user interface should be flexible for a broad range of use cases.

5.7 Notifications and Alarms

Notifications and alarms are a core function of the spectrum monitoring system. Similar to user interface considerations, notifications and alarms should also be easy to be understood by an operator who does not have spectrum monitoring data analysis experience. Some operators may want the alarm to be displayed on a screen (if the station is attended), while other operators may want the alarm passed to the central station (if the alarm occurred at an unattended station). Other forms of alarms such as sending a text message to a designated operator should also be available. When an alarm occurs, the monitoring system should be set up to start a new measurement for a detailed examination of the frequency that triggered the alarm.

Moreover, the content of notifications and alarms should be related to the application case and reflect the situation effectively. Some exemplary indicators to be shown can be density rate of the corresponding frequency band and related interference or power levels of other signals. If these parameters exceed threshold levels, then certain alarm mechanisms should be operated.

5.8 Historical Database

The spectrum monitoring system should record spectrum utilization for long periods of time - months or years which would permit robust post-processing. This information can be used to analyze spectrum use trends and document what portions of the spectrum are in use in a given area, including how the signal strengths of various signals change over time. Instead of sampling the signal strength, recording of the RF spectrum is crucial because once recorded, there is essentially no limit to the variety of ways the data can be analyzed to understand how the spectrum is being utilized and locate the source of a rogue emitter more effectively. Measured values, statistics, graphics, and frequency lists should be saved to an internal database and the system should be configured for local and/or central site databases. The database information should be exported in standard formats such as plain text comma separated values (CSV), binary file for all Microsoft Excel spreadsheets (XLS), or extensible markup language (XML) which is used to annotate text and the operators should be able to integrate their own database information. Permissions on who can access the database and what can be done to the database should be configurable as well. Therefore, recording each measurement in a database and collecting all measurement results are beneficial for comprehensive modeling of long-term system performance, especially for dynamic industrial environments.

5.9 Industrial Control System Integration

Spectrum monitoring systems should provide RF situational awareness information to an industrial control system (ICS) environment through a spectrum management discipline. In spectrum management applications, the designated Spectrum Manager should create a list of all known emitters in a given area. This frequency list becomes the baseline. As the spectrum is monitored, or new RF devices are introduced, proper frequency planning is required to ensure spectrum integrity.

Spectrum management in Internet of Things (IoT) should provide dynamic spectrum access for field devices which means that the spectrum allocation will differ in time and space based on the regional and temporal spectrum use knowledge, relying on rapid and true awareness of the spectrum situation [3].

The IoT concept is expected to be used in various applications due to usage of low-cost devices and functional communication abilities. In accordance with this trend, IoT is also considered for industrial usage and this concept is called Industrial IoT (IIoT). Usage of sensors or low-cost wireless devices in industrial facilities has been increased significantly because of their ease of configuration. Control systems monitor production processes in the industrial environments and sensors have a key role in such systems. Therefore, control systems should be evaluated with the IoT concept and its requirements. Such IoT usage is being implemented even now in control systems such as heating, ventilation and air conditioning (HVAC) systems, asset management, and tracking some other systems utilized in factory automation or smart grid. As an important issue, usage density of IoT devices will increase spectrum demand. In order to keep networks stable, spectrum management will be crucial for industrial applications. Therefore, spectrum monitoring will be an essential functionality for such situations. It is important to decide how to add such monitoring functionality into a network. IoT devices have limited hardware functionalities and may not have monitoring capability. As the first step, a separate monitoring node should be used and spectrum decisions should be shared with IoT devices. According to a recent report in [4], high-quality software defined radios (SDRs) are used in the Netherlands as monitoring nodes. These SDRs can be configured to collect data on specific frequency bands in specific time frames. As the second step, IoT devices should change their frequency channel according to spectrum monitoring results and empty channel decisions. This functionality can be provided with a Medium Access Control (MAC) protocol, which is used to provide the data link layer of the Ethernet local area network (LAN) system, included in devices, and even today, low-cost devices can support such a property. The database is constructed by gathering the information from the monitoring nodes, which reads the MAC address in a packet and uploads the MAC address information and received power information to the database. Based on the constructed database, the spectrum manager that is connected to the database, selects a suitable channel for a spectrum shared distributed network with avoiding mutual interference. Thus, integration of control system components with spectrum monitoring can be realized with a simple MAC protocol or with a similar process.

6 CONCLUSIONS

The RF spectrum is a limited natural resource that requires rational allocation and monitoring techniques that keep pace with the growing demand. The necessity for spectrum monitoring solutions, originally used primarily for regulatory and government use, is now finding its way into commercial applications such as service providers and industrial applications.

Disruption in the RF spectrum can contribute to productivity or monetary losses as well as create safety concerns in the industrial environments. While most RF interferers are unintentional such as faulty or new installations of nearby equipment, the increase in the technology to disrupt or exploit RF communications is contributing to intentional acts (i.e., RF jammers or the use of RF based devices such as civilian remote control (RC) drones to exploit targets of interest).

We have described spectrum monitoring requirements of industrial facilities, and the technologies based on the distributed RF spectrum sensor units which would improve the spectral analysis by creating a correlation between the measurement data from the different sensor units. In addition to identifying spectrum monitoring requirements, this document is a starting point for developing a prototype for spectral analysis in industrial facilities, including indoor/outdoor plants and factories.

BIBLIOGRAPHY

[1] Dave Lavinsky, “The Two Most Important Quotes In Business.” [Online]. Available: http://www.growthink.com/content/two-most-important-quotes-business. [Accessed: 15-Dec-2016].

[2] International Telecommunication Union (2015). *Spectrum monitoring evolution* 2015. Retrieved August 10, 2017 from https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2355-2015-PDF-E.pdf.

[3] H. Ning, *Unit and Ubiquitous Internet of Things* (2013), 187-199

[4] Tommy van der Vorst, Jasper Veldman, and Jan van Rees, “The wireless Internet of Things : Spectrum utilisation and monitoring,” August, 2016.

[5] “Ethernet-to-the-Factory 1.2 Design and Implementation Guide.” [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG.html. [Accessed: 20-Dec-2016].

[6] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security,” National Institute of Standards and Technology, Gaithersburg, MD, 2015.

Annex A. Industrial Control Systems

Industrial control systems (ICSs) are command and control networks designed to monitor and control a variety of industrial processes, such as discrete manufacturing, gas and electricity distribution, water treatment, transportation, oil refining, beverage factories, or chemical production.

The following components make up an ICS:

- **Data Historian:** The data historian is a database for recording and retrieving process data to analyze the plant operation.
- **Sensors and Actuators:** They are used for interaction with the physical world, for example, pressure sensor, valves, motors.
- **Local Human-Machine Interface (HMI):** HMI consists of hardware and software that provides a visual representation of a control system and real time data acquisition.
- **Main Supervisory Screen:** It is used for remote supervision of the entire industrial process
- **Programmable Logic Controllers (PLCs):** A PLC is an industrial computer with digital and analog I/O modules, communication modules, processor, and power supply, forming the building block of the industrial control networks.

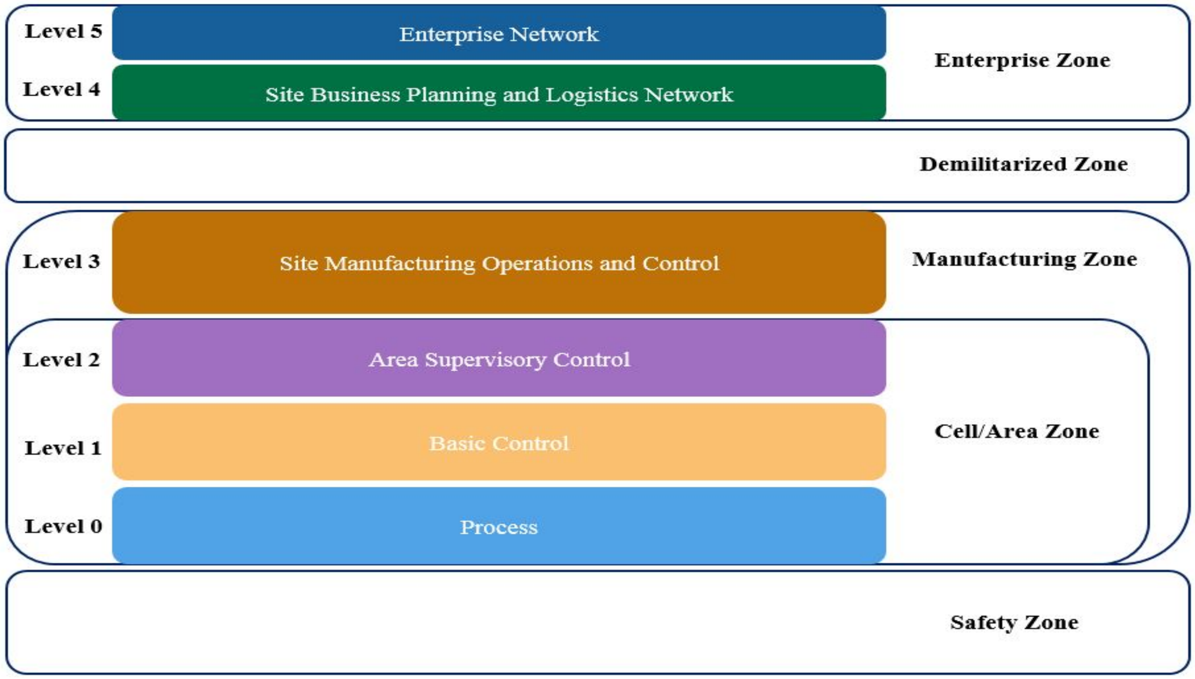

Figure A.1. The Purdue Reference Model for Industrial Control Systems

The International Society of Automation (ISA)-99 Committee for Manufacturing and Control Systems Security has identified the reference architecture for ICSs shown in Figure A.1 to systematize control system functions.

The zones and levels of operations in this plant logical framework are given in detail in Table A.1.

Table A.1. The Purdue Reference Model Zones and Levels for Control Hierarchy [5]

Enterprise Zone		
Level 5	Enterprise	Corporate IT infrastructure and functions such as resource management and virtual private network (VPN) remote access.
Level 4	Site Business Planning and Logistics	This layer is an extension of the enterprise network and includes IT systems such as plant reporting (inventory, performance) and operational and maintenance management.
Demilitarized Zone		
	DMZ	This layer controls the data traffic between the manufacturing and enterprise zones providing a buffer zone.
Manufacturing Zone		
Level 3	Manufacturing Operations and Control	This layer is responsible for a site manufacturing operation to produce the desired end product.
Cell/Area Zone		
Level 2	Area Supervisory Control	This layer includes the functions for the runtime supervision such as HMI, and alarms/alert systems.
Level 1	Basic Control	This layer has process control equipments, such as PLCs and remote terminal units (RTUs).
Level 0	Process	This layer has sensors and instrumentation elements to monitor and control the manufacturing process.
Safety Zone		
		The layer has systems which monitor processes and return processes to safety if they exceed a defined threshold value.

Figure A.2 shows a spectrum monitoring system operating on the basis of distributed RF spectrum sensor units, working together in a coordinated way to detect and confirm anomalies in the spectrum.

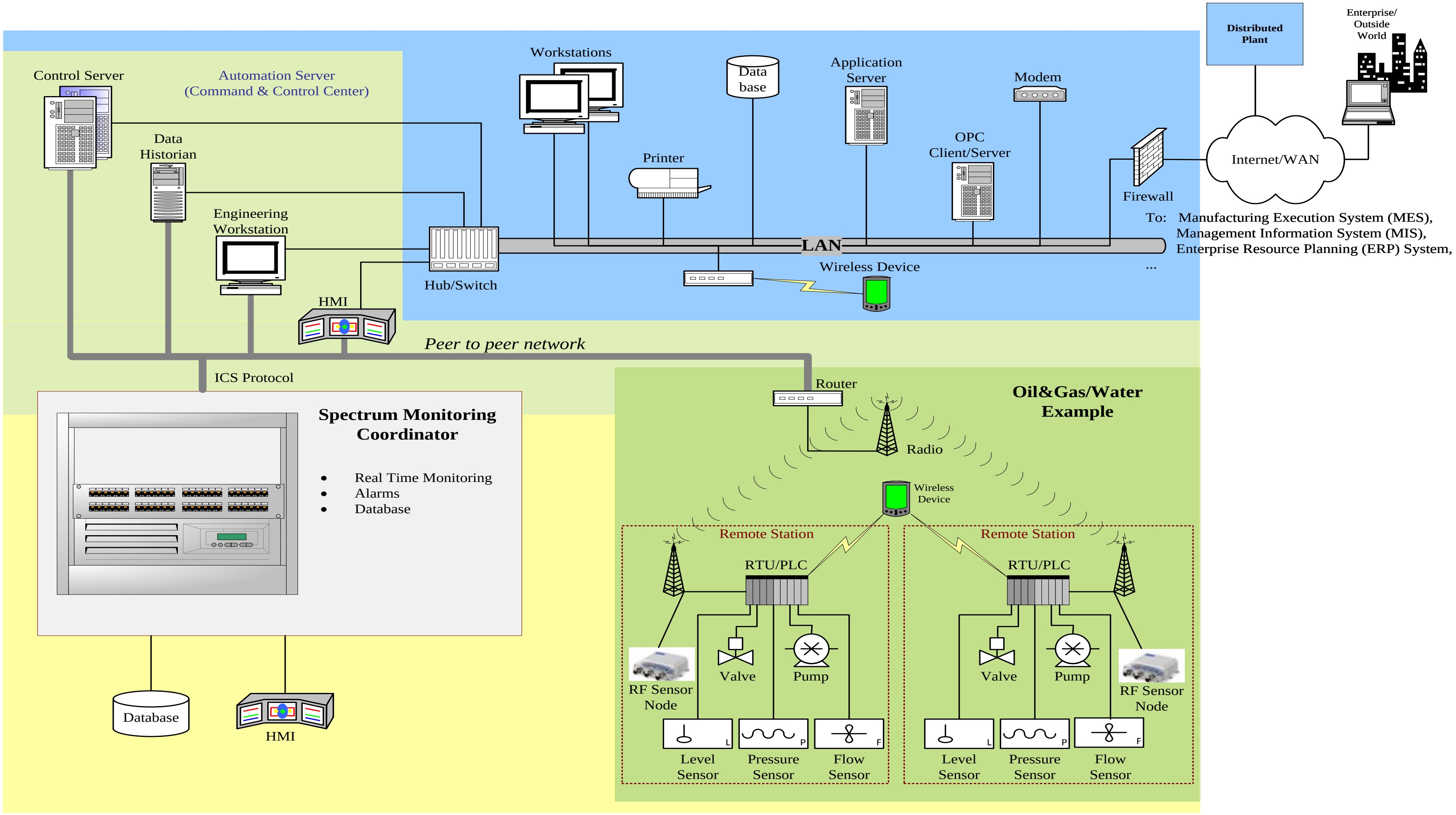

Figure.A.2. Industrial Control System with Spectrum Monitoring Overlay [6]