A Practical Guide to Locate and Mitigate Interference

In the crowded RF spectrum environment, it is critical to detect, identify, locate, and mitigate problem signals before they impact communications

eBook

KEYSIGHT

Optimize and Protect Your Communication Systems with the Right Knowledge and Tools

A seemingly limitless variety of wireless systems operate in the world today, with new ones continuously emerging. Governments around the world do their best to regulate the electromagnetic (EM) spectrum, assigning specific frequency bands to certain communications applications. As these frequency bands become more crowded, networks are more likely to experience interference or even communications failure. These challenges arise from any radio-frequency (RF) system, including cellular phones and drones.

These intentional or accidental signals can wreak havoc on a wireless system, creating issues such as noise in the channel or even loss of service. Spectrum monitoring continues to evolve to better detect and locate interferers in cellular and satellite communications while reinforcing key tactics to mitigate interference.

In today's crowded RF spectrum, interference is a frequent and unpredictable threat to performance and security. You need tools to help you detect, classify, and locate it quickly and accurately.

Key Trends

Detection and mitigation of problem signals continue to evolve because of the following trends:

1. Continuous appearance of interferers as new communication services launch
2. Proliferation of increasingly complex, difficult to detect signal events
3. Challenge to stay at least one step ahead of potential interference problems

In this eBook, we explore these areas and delve into ways that spectrum monitoring and signal analysis techniques continue advancing to safeguard communications.

Contents

CHAPTER 1

Types of Interference

CHAPTER 1

ABCs of Interference

There are two types of interferers — in-band and out-of-band. In-band interference occurs when a transmitter operates directly on top of another signal at a particular frequency. Usually, you can identify those emitters more easily than out-of-band interferers.

With out-of-band interference, a transmitter activates at a different frequency from the "victim signal" — the one affected by the interfering signal. When the out-of-band transmitter activates, it has intermodulation distortion or harmonic mixing. This may cause it to mix with another nearby signal or even the receiver itself. If the impacted receiver acts as a mixing receiver, it creates a harmful interference signal on the frequency. Increasingly varied sources of interference exist in the RF spectrum, yet signal issues usually stem from the following set of culprits: cellular communications, satellite interference, and unlicensed devices.

Cellular Communications

Cellular communication experiences both in-band and out-of-band interference. In some scenarios, it causes both types of interference. Today's cellular systems operate at a lower power level because of the large number of deployed base stations. Unless a device is a long distance from a base station, it will not transmit at very high power. Because today's cellular devices adjust their power based on their proximity, a fairly low-power interferer can be problematic for some of these lower-power devices.

Cellular and Spectrum Sharing

Cellular technologies also introduce interference issues related to spectrum sharing, whereby multiple services occupy the same frequency band. Much of 5G will deploy in bands previously used for military systems, such as the Ka-band for radar and satellite services. In lower-frequency 5G frequency ranges like FR1, for example, the C-band's small aperture terminals (VSAT) already operate in a similar or adjacent band around 3.5 GHz. If you have a 5G base station located in the azimuth beam of a VSAT terminal blasting in an adjacent band, it could bleed over. The result increases the effective or ambient noise for that C-band terminal, potentially causing harmful interference.

As regulatory authorities allocate frequencies for 5G in FR1, they need to consider existing C-band satellite services in urban environments. Frequently, those belong to critical services like government communications. The regulatory authority must carefully choose where it positions base stations to prevent these issues.

Satellite Interference

Beyond cellular communications, satellites support many other applications. A diverse range of systems now relies on Global Navigation Satellite Services (GNSS) such as the Global Positioning System (U.S.), GLONASS (Russia's GNSS), Galileo (the European Union's GNSS), and BeiDou (China's GNSS).

Interference poses a risk to the performance of various systems that depend on precision timing. Solutions available today specifically tackle satellite interference. By setting up spectrum monitoring and signal analysis sites around the world, they locate issues such as industrial interference on satellite systems. To precisely geo-locate an interferer, however, they need to hand off to a terrestrial system.

Unlicensed Devices

In today's global economy, consumers frequently bring unlicensed devices from one country to another. Although these devices comply with spectrum rules at home, when used abroad, they can interfere with wireless services in the host country.

An example is digital enhanced cordless telecommunication (DECT) 6.0 phones, which are popular in U.S. homes and businesses. These phones work well in terms of the wireless connection between the handset and base station. When users turn their DECT 6.0 phones on, the devices emit in the personal communication service (PCS) wireless cellular band. Several countries have reported issues with those phones interfering with the cellular network.

Non-Usual Suspects

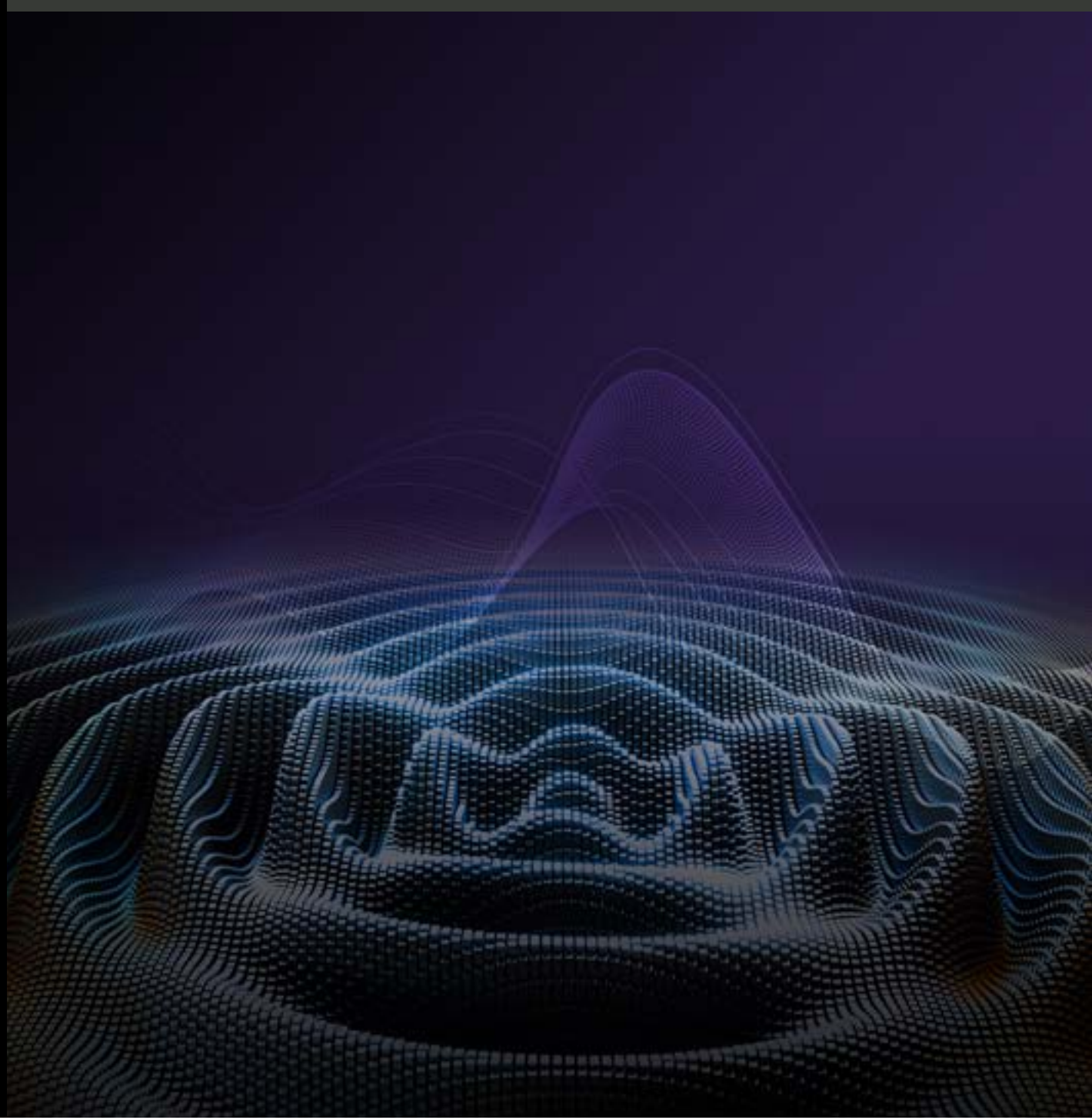
The prevalence of technology and communications in today's world creates an increased chance of interference issues. Some of these examples comprise non-communication sources of interference. Light-emitting diodes (LEDs), for example, can affect the reception of FM radio, digital television (DTV) broadcast, very high frequency (VHF) communications, and Long-Term Evolution (LTE) cellular up to 300 meters.

Other common problem sources include active indoor DTV receiving antennas and amplifiers. They may impact aeronautical communications, police/fire/rescue, and Global System for Mobile Communication (GSM) / Universal Mobile Telecommunications System (UMTS) cellular up to two kilometers or greater if connected to an outdoor aerial antenna.

Switching power supplies can influence VHF radio communications up to 50 meters. Even electronic signs present potential interference problems, impacting LTE cellular communications to 200 meters. To mitigate any risks arising from these signal sources, you need to first prevent or isolate interference.

CHAPTER 2

Mitigating Interference



CHAPTER 2

High Stakes Call for Mitigation

To mitigate risks in communications, you need to prevent or isolate interference in a crowded spectrum. For example, in a theme park or stadium, police, staff, and medical professionals communicate by radio when someone needs help or other issues arise. Such environments are at capacity with people using their own devices to make calls, post on social media, or send text messages. An interfering signal could potentially take out the emergency communications in a stadium.

People carry a variety of portable devices. The following are some devices that can impact your network:

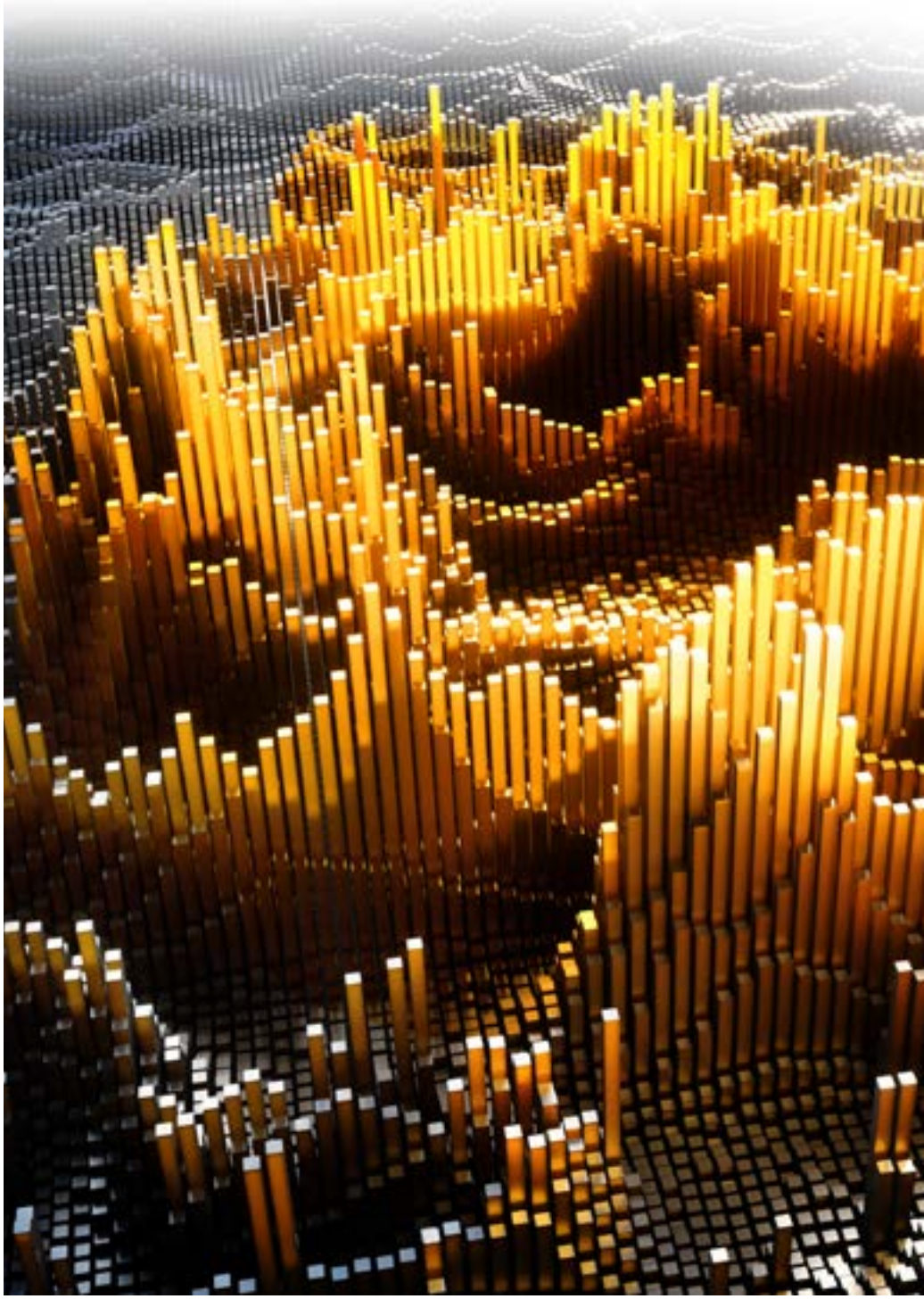
- cell phones with different antennas to support Bluetooth, Wi-Fi, and various cellular standards
- an automotive key fob that uses an RF signal to control vehicle access
- earbuds
- two-way land mobile radios to use for emergency response staff in the field

Monitoring and Analysis Fundamentals

Mitigating interference requires spectrum monitoring and signal analysis. For applications such as interference detection, engineers perform these steps in situ — often in dense signal environments. Monitoring does not usually take place in a chamber, but out in the real world like on a rooftop with an antenna. As a result, you cannot control what the receiver sees and needs to record, trim, and process the signals of interest.

Smart, distributed RF sensing lets you move away from traditional direction-finding techniques for emitter location. Signal analysis and spectrum monitoring, once primarily a function of hardware, are now done using software. Today, new and unique ways of collecting and storing spectral data allow engineers to visualize it in novel ways and take new actions based on information regarding spectrum activity.

Monitoring and analysis systems perform three necessary measurements: energy detection, signal classification, and emitter geolocation. These functions provide guidance and assistance on issues regarding the International Telecommunication Union (ITU) / regulatory, spectrum security, or monitoring / intercept. The following applications increasingly call for spectrum monitoring and interference detection: facilities monitoring, satellite / outdoor ranges, drone monitoring, and signal intelligence.



Signal Detection

Finding the source of signal interference is difficult. The following are two different approaches to detecting signals:

1. RF sensors/fingerprinting

One method is to place time-synchronized RF sensors around the area of concern. A central control facility collects and analyzes data from these sensors. The software detects, identifies, and provides the location of interfering signals using a unique RF fingerprinting algorithm. Discovery of that fingerprint anywhere in the spectrum triggers geolocation, which leads to the emitter location. Imagine the shoreline of a lake; this process is much like measuring the ripples coming onshore in varying lengths after you throw a rock in the water. The sensors — gathering the information at the shoreline — can pinpoint where the rock hit the lake.

2. Handheld analyzer/geolocation software

Another step involves using a handheld analyzer in conjunction with the geolocation software. A geolocation algorithm can pinpoint the location of the interfering signal down to less than 100 meters, but you still need someone in that location with an instrument for those last few meters. A handheld analyzer with a directional wand antenna pointed in different directions will pick up the strongest signal. Determining the source of a moving signal, such as something transmitting from a vehicle, is a bit trickier. With continuous monitoring and geolocation, it is possible to determine the direction and speed of the moving signal.

To identify a transmitter, you also can make a recording of it. A quadrature signal (IQ) recording gives you all the information about that signal. You can leverage software to utilize that recording across various applications, driving it into different products. For example, signal analysis tools enable you to identify whether it is a signal appearing in the wrong band.

The Drone Challenge

Drones are increasingly popular as toys and for industrial uses. They pose threats in several different ways. As drones become cheaper, smaller, and more prevalent, someone can use them to observe a targeted location, carry drugs across a border, or even drop a dangerous substance onto a crowd or area. It is critical to be able to locate both the drone and the controller.

Drone detection consists of the following steps:

1. Detect the presence of the drone and the controller.
2. Identify the type of drone including the make and model.
3. Pinpoint the drone's location using a direction finding or geolocation algorithm.
4. Implement a mitigation approach according to the scenario (for example, preventing drones from flying over sensitive / classified areas).

Whether the intent is harmless or not, today's inexpensive and accessible technology results in increased signal events.

CHAPTER 3

The Presence of Elusive Signals

CHAPTER 3

Hidden Signals

Often, an interferer no longer appears when the equipment is set up to detect and locate it. Interferers are a common example of these elusive signals. They may affect communications — especially clarity or audibility of sound — by creating noise or distortion. Some signal events are elusive in a different way: they only occur occasionally.

As the increasingly crowded spectrum results in more elusive signal events, new strategies are needed to detect, classify, locate, and mitigate interferers.

How Signals Hide

If a system and the interferer are on the same frequency, nothing appears wrong on a spectrum analyzer. The two signals appear right on top of each other, like one normal signal. Yet interference often reveals itself by affecting audibility and clarity via noise or distortion.

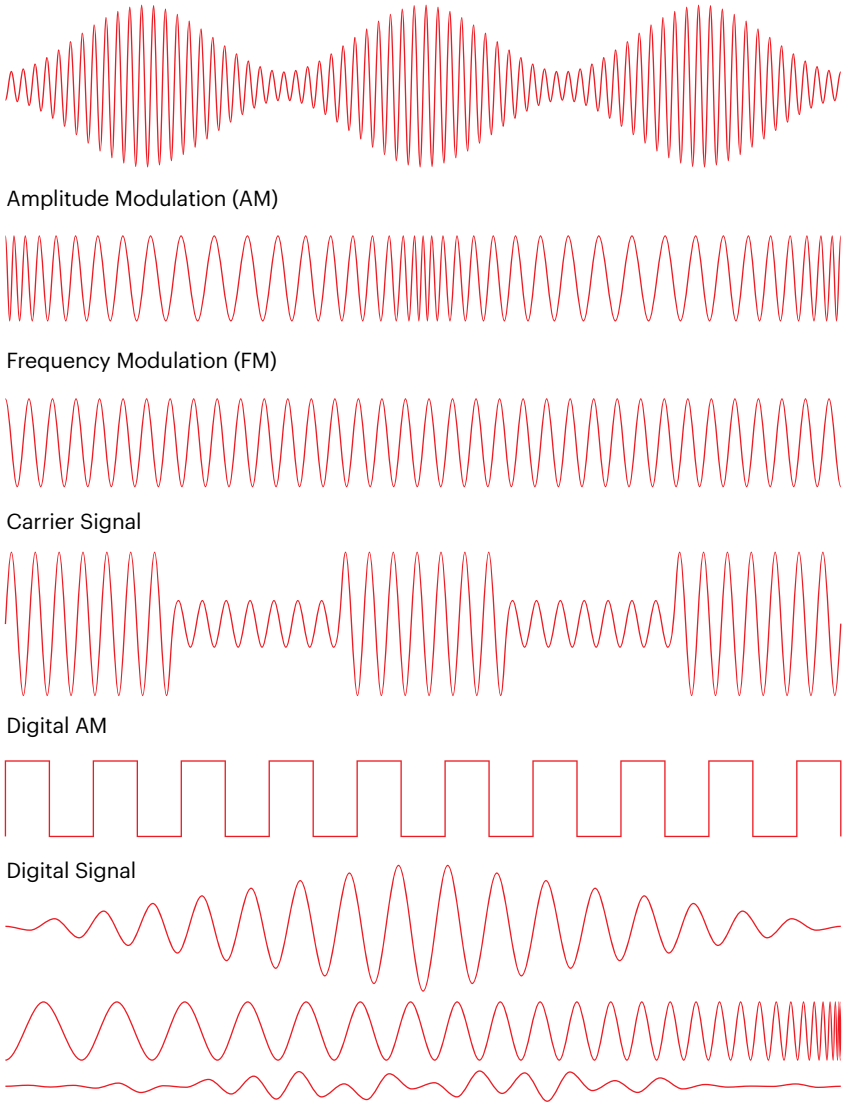
Other signal events are elusive because they rarely occur, maybe once a month or year. Yet they still can cause significant problems, depending on their frequency. Even if an interfering signal event occurs only once a year, it could negatively affect mission-critical systems like emergency services or early-warning systems.

From traditional swept heterodyne methods to sensors and fast Fourier transform (FFT) approaches, evolving spectrum monitoring methods more effectively detect, identify, and report on these hard-to-find signals to ensure better communications.

Two Common Modes of Operation

To maintain awareness of elusive or problem signals, engineers looking to perform spectrum monitoring follow one of two approaches: survey or search. With the first method, the engineer surveys the spectrum to determine what signals occur in an environment. The engineer can then create a table of frequencies, bandwidths, and modulation types. Those coming to a new area to erect a tower use this “spectral survey.”

The second approach — search — is trickier. Here, the engineer usually watches a specific signal because of information that is already known. For example, who is the owner or who is using it? The search could focus on an individual’s cell phone number or devices in use. The user or agency performing the search preloads that information into a system and tells the system to find those elements. If the system detects that signal, it sends an immediate notification.



Finding that Elusive Signal Event

To detect and identify an elusive signal, begin with the environmental scan or survey to determine what signals are in the environment. Frequently, engineers have already documented the signals they are broadcasting or using and know which channels are effective versus the ones that exhibit issues. Problems usually show up in a specific frequency or channel.

You can use that information to focus your survey on that area of the spectrum. With a spectrum analyzer, you may not see the interfering signal if it is riding right on top of the signal for which you are searching. When everything appears fine, but performance issues clearly exist, the next step is to deploy sensors around the area. By placing four or five sensors a mile or so apart, for example, you can perform the same survey again in that frequency band.

Take the Right Approach

Sensor and geolocation data often reveal more details around what is occurring in the spectrum environment. For example, the data may show two locations for the same frequency, which makes it more likely that one of them is causing the interference. Consider what is at each location, such as a tower or transmitter. A location not documented as the source of any signals is likely the source of interference. Sending engineers to the point of interference to gather more information on the source is the most expensive step.

You can accomplish signal identification in the initial survey by looking at the frequency spectrum. If you know how the signal should appear, you can recognize a different signal immediately. It might have a different modulation type or shape in the spectrum. Occasionally, such visual clues help easily discern the source of the signal — especially given the knowledge of the signals in the broader environment, thanks to the initial survey. Consider such issues at the beginning of the process to determine the best spectrum monitoring approach to apply.

Pluses and Minuses to Different Approaches

Initially, spectrum monitoring used a swept heterodyne front end. It looked at one very narrow chunk of the spectrum at a time, moving across the frequency band of interest — like looking through binoculars. The user would move the binoculars from left to right, which limited the information gathered to the contents of the lens view.

Newer swept-mode analyzers use an increasingly wider stare in that binocular view. Yet the old approach still offers advantages. The swept heterodyne approach looks at a narrow chunk of the spectrum. It contains less noise, making it possible to discern some lower-amplitude signals.

Choose the Best Trade-Off

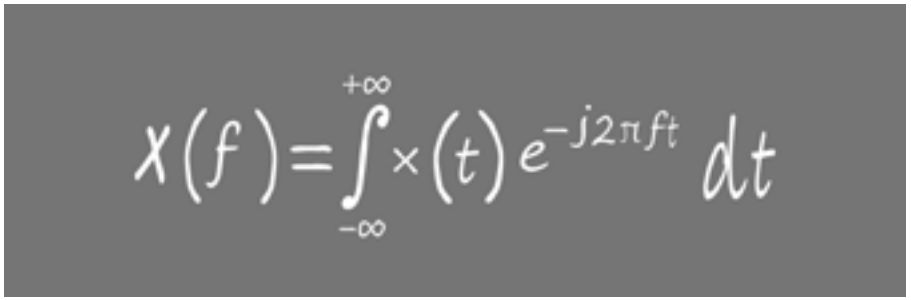
Spectrum monitoring requires constant trade offs between dynamic range, wider bandwidths, and sweep speeds. Just because technology allows you to grab a gigahertz of the spectrum, it might not be the best approach. A larger and wider chunk of the spectrum means more environmental noise. The noise floor rises, limiting the selectivity or sensitivity of the front end. You will then struggle to single out signals that might be miles away.

However, dynamic range is not an issue if the problem signal you seek is fairly high in amplitude and causing problems across the board. With a high-amplitude signal, you can simply grab a huge chunk of spectrum. The noise floor is not a concern, as the problem signal will show in that wide chunk of spectrum. In contrast, if a low-amplitude signal is causing problems, you can divide the spectrum into smaller steps. This approach reduces the noise floor, making the signal visible.

Spectrum monitoring requires constant trade offs between dynamic range, wider bandwidths, and sweep speeds.

Improvements via Fast Fourier Transform

The noise floor is lower using a fast Fourier transform (FFT) approach with more processing power. An FFT is a series of mathematical equations used to emulate the frequency spectrum. A sufficiently large FFT reduces the spacing between each frequency point, lowering the resolution bandwidth and the noise floor to provide a high dynamic range and faster sweep speeds.



With a 1 kHz resolution bandwidth (RBW), it is possible to see signals spaced 1 kHz apart. Achieving a 1 kHz bandwidth across 1 GHz of stare bandwidth requires a huge FFT (100,000 points). You can increase the RBW

to 1 MHz. However, all the signals in a 1 MHz band are combined into a single point on the spectrum. So instead of seeing 100,000 signals, you see only 100 signals. Larger FFTs provide a narrower resolution bandwidth even with a wide bandwidth stare. To summarize, the lower the resolution bandwidth, the lower the noise floor, and the more sensitive the front end.

Choose the Right Approach

Assume you want to monitor 100 MHz of spectrum using an RF sensor designed for measuring signals off the airwaves with a 20 MHz stare (instantaneous) bandwidth, for example. It will take five steps to cover 100 MHz. To determine whether an FFT or other spectrum monitoring approach would be best, consider the following:

- Can you look instantaneously at a big chunk of the spectrum?
- Do you have the ability to step through that spectrum quickly?
- What is your probability of intercept?
- Given the sweep speed, how quickly can you cover the area in the spectrum of interest?

CONCLUSION

Prepare for the Future

CONCLUSION

Prepare for the Future

No matter the approach, spectrum monitoring is a critical aspect of safeguarding spectrum and communications systems. More organizations now opt for ongoing spectrum monitoring rather than just bringing in such capabilities when problems arise. Spectrum monitoring software automates signal search and survey functions. It provides a complete signal monitoring solution when combined with hardware such as an RF sensor, vector signal analyzer (VSA) modules, or handheld RF analyzers.

With the ever-changing RF environment, finding and mitigating one problem does not mean there will not be others. It is best to be prepared for when a signal that causes a problem appears, so you can quickly locate it and find the cause.

To learn how spectrum monitoring and signal analysis are evolving to confront challenges ranging from evasive signals to interferers, we offer a range of white papers:

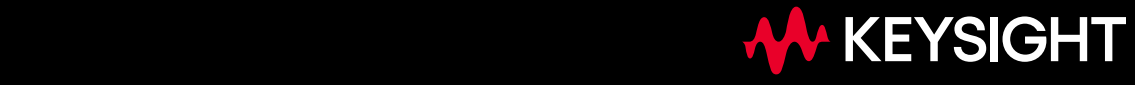
- Monitor Your RF Spectrum for These Three Signal Trends
- Use Spectrum Monitoring to Combat Elusive Signals
- Combat Interferers with RF Spectrum Monitoring
- Monitor Your RF Spectrum for Threats

An additional white paper offers tips on successful signal development:

- New Tools Aid Signals Development.

For information on how Keysight supports spectrum monitoring and signal analysis, visit our site.

Click here to get a free trial of Keysight's N6820ES Surveyor 4D spectrum monitoring software. Surveyor 4D software operates with the N6841A RF Sensor, the M9391A or M9393A PXI vector signal analyzer (VSA) modules, and the FieldFox handheld RF analyzers.



Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.