Electronic Design

STEVE TARANOVICH, Contributing Editor

EMI and Surge Protection in the IIoT

Since many more devices are wirelessly connected, spectral noise level increases and, as a result, it causes radio interference between IIoT devices.

The industrial Internet of Things (IIoT) is an amazing network of connected devices within modern industrial sectors. It's composed of myriad connected devices, both wired and wireless, in industrial complexes. However, since many more devices are being wirelessly connected, the spectral noise level increases as does the radio interference between IoT devices.

In the last 30 years, many of the main processes that haven't yet been fully automated are the integration of logistics, material handling, and factory automation. This remaining integration is best being achieved by adding wireless technology in Industry 4.0.

Industry 4.0 is revolutionizing the automation, analysis, and monitoring of supply chains through smart technology. Industry 4.0 is powered by the IIoT and cyber-physical systems, which are smart, autonomous systems employing computer-based algorithms that monitor and control physical assets such as robots, machinery, and vehicles.

Wireless technology is already being used for industrial production in some select, non-critical applications. In today's industrial environment, advanced, smart wireless technology is finding its way into mission-critical tasks. Surveys say that the most diverse wireless technology in industrial production is Wi-Fi.

Shown is one type of a Surge Protection Device (SPD). (Utmel Electronic)

Enter Radio-Frequency Interference

Radio-frequency interference (RFI) and electromagnetic interference (EMI) are typically used interchangeably since radio waves are simply a subset of the electromagnetic spectrum. In actual practice, EMI refers to short-range interference that's caused by high-frequency emissions within a device itself. RFI refers to longer wavelength interference from sources external to a device.

Wireless communications systems have successfully removed the physical barriers of traditional wired communication architectures, with a side benefit of lower cost. These wireless systems are easily deployed, need little maintenance, and have quite good flexibility.

The caveat here is that all of these wireless technologies use the unlicensed frequency bands, such as the industrial, scientific, and medical (ISM) band. The ISM band needs no licensing. RFI management is not only challenging due to its noise level and heavy usage, but also because all of these different standards are operating in parallel.

A big problem exists—the legal limit to how much radiation is emitted by unlicensed bands. As a result, range and wall penetration of the radiated power is very low. Unfortunately, the use of unlicensed spectrum for industrial applications will most likely not

satisfy the demanding quality requirements of the IIoT.

To achieve and satisfy those demanding quality needs, the industry is counting on 5G technology. It was actually designed to be the new standard for industrial connectivity.

5G offers a variety of optimal configurations for usage scenarios identified by the ITU-R:

- Enhanced mobile broadband (eMBB)
- Massive machine-type communication (mMTC)
- Ultra-reliable low-latency communications (URLLC)

5G employs licensed frequency bands. In Europe, the carrier frequencies planned for 5G networks are 700 MHz, 900 MHz, 2100 MHz, 3.5 GHz, and 26 GHz. Even if these bands all fall outside of the ISM bands, and 5G networks manage frequencies centrally, they still need to coexist with legacy systems.

If there's no proper filtering for each band, emissions from intermodulation products, or spurious or out-of-band emis-sions, may produce spurs outside the allocated channel. De-signers need to investigate the possible interference between 5G networks and legacy radio systems on the industrial shop floor.

Investigators used SEAMCAT, an agnostic simulation tool that can assess RFI between three wireless communication systems commonly used on the factory shop floor (Wi-Fi, Bluetooth, and WirelessHART) and a 5G network.

The results, from the three interference scenarios mentioned above, have proven that from an electromagnetic point of view, interference levels will affect the receiver of legacy systems, 5G user equipment (UE), and 5G base stations (BS) differently. It also can affect their performance.

In simulated scenarios, legacy systems were more prone to be affected by interference from other legacy systems working in co-channel arrangements (e.g., 2.4-GHz ISM band) than from 5G networks using the adjacent channel n53. When the 5G network is simulated as the system that's suffering RFI, legacy systems produce a higher degradation in the UE uplink channel—maximum bit-rate loss was 12% with Wi-Fi as the interfering system.

Surge Currents and Surge Protection Devices

Surge currents

Surge currents are sudden spikes and drops in voltage beyond what's considered normal for electronic/electrical equipment. Inrush current contributes to this problem; however, it will occur mostly when a device is first powered on. This effect will crop up in both ac and dc circuitry.

Surge protection devices (SPDs)

SPDs are indispensable in protecting electrical installations (consumer unit, wiring, and accessories) from electrical power surges known as transient overvoltages *(see figure)*.

These devices are critical in protecting electronic equipment, especially from lightning. The SPD comes in the following types:

- *Voltage switch:* In the absence of transient overvoltage, this SPD will exhibit high impedance. When the device responds to a lightning transient overvoltage, its impedance changes to a low impedance, enabling the lightning current to pass through the device. This is also known as a "short-circuit switch type SPD."
- *Pressure limiting:* In the absence of any transient overvoltage, this SPD will exhibit a high impedance. As the surge current and voltage increases, the device impedance will continue to decrease, and its current and voltage characteristics will be quite nonlinear. Sometimes referred to as a "clamped type SPD."
- *Combination:* This device combines voltage-switching and voltage-limiting type components. It may be displayed as a voltage-switching type or a voltage-limiting type, or both, depending on the characteristics of the applied voltage.

What are Transient Overvoltages?

Transients in electrical networks occur very quickly—in fact, it's so fast that most times they can't be observed.[2] The effect of transients on an electrical network can be costly, and sometimes devastating, to the electrical power-distribution system. Transient types include:

- *Oscillatory transients:* These are sudden changes in voltage that oscillate at the natural frequency. They will usually decay to zero in the same cycle. Such transients will typically occur when switching a capacitive load off (usually that load might be a capacitor bank).• *Impulsive transients:* These kinds of transients will be seen as sudden peaks in voltage or current levels, in either the positive- or negative-going direction. They can be seen as either fast, medium, or slow events, which will depend on their rise time from nominal to peak voltage. One of the main causes of these transient types is poor grounding, and that will lead to impulsive transients. Other causes of such transients can be lightning or switching on quite a few inductive loads, like motors or electrostatic discharges (ESDs), all at once.

Intentional Electromagnetic Interferences (IEMI)

During a 1999 workshop in Zurich at an EMC Symposium, a widely accepted definition of IEMI was defined as: "Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes.[3]"

IEMI is actually a cyberattack because it targets "cyber" elements like computers, networks, and devices. This isn't "cyber" in the sense of being a digital attack that directly manipulates 1s and 0s. Instead of the manipulation of 1s and 0s,

IEMI focuses on analog interference with the electromagnetic (EM) signals that are commonly used in our electronic devices and communications.

To help prevent an IEMI attack, here are some countermeasures:

- Proper grounding of equipment
- Distance: EMI falls off as the square of the distance between the intentional interference and the IEMI directed at targeted devices
- Shielding
- Filtering
- Use of fiber optics

Summary

An SPD is an indispensable device used primarily for lightning protection of electronic equipment. The SPD function is to limit the instantaneous overvoltage of power lines, as well as signal transmission lines, to the safe operating voltage range that the equipment or system is able to withstand. The SPD can discharge powerful lightning currents into the ground to protect equipment or systems from damaging shocks.

References

1. Electromagnetic Interference Analysis of Industrial IoT Networks: From Legacy Systems to 5G, 2020.

2. Transient Over-voltages in Power System Causes, Types and Effect on Power Quality, Asia Power Quality Initiative (APQI), 2019.

3. The Growing Threat of Intentional Electromagnetic Interference (IEMI) Attacks, Marin Ivezic, 2018.