Electronic Design

By STEVE TARANOVICH, Contributing Editor

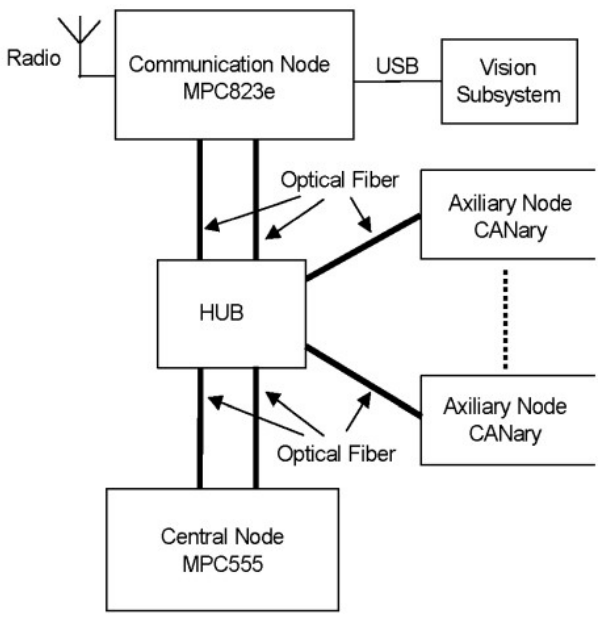
Preventing Intentional EMI—aka Sabotage

IEMI from high-power microwave sources and EM pulses can generate significant threats to electronic systems in civil and infrastructure. Thus, inclusion of methods that recognize and reduce IEMI in designs is more critical than ever.

Before we can define intentional electromagnetic interference (IEMI), which will also be referred to as "sabotage" in this article, let's begin by characterizing electromagnetic waves.

A mechanical wave can be defined as a vibration or disturbance in matter through some medium (such as a solid, liquid, gas, or plasma). Sound waves occurring in the air are mechanical waves.

A changing magnetic field induces a changing electric field and vice versa—these two are linked. The two changing fields ultimately will form electromagnetic waves. Electromagnetic waves aren't like mechanical waves; they don't need a medium to propagate. Thus, electromagnetic waves have the ability to travel not just through air and solid materials, but through the vacuum of space as well.



1. This is the distributed control architecture for a robot design. (Image from Reference 11)

An electromagnetic wave also is described in terms of its energy; that is, in units of measurement known as electron volts (eV). The electron volt is defined as the amount of kinetic energy necessary to move an electron through a 1-V potential. When energy moves along the spectrum, from long to short wavelengths, that energy will increase as its wavelength shortens.

IEMI Definition

During the Zurich EMC Symposium in February 1999, the International Electrotechnical Commission (IEC) proposed the definition of intentional electromagnetic interference (IEMI) as:

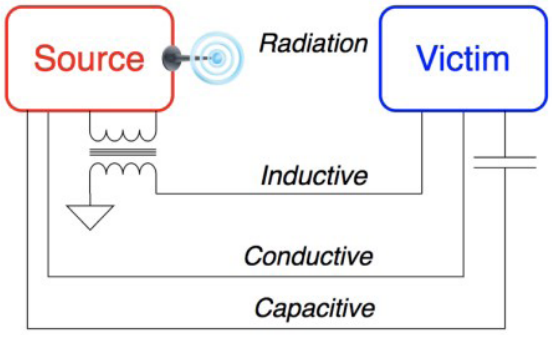
"The intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes."

Therefore, systems may be greatly disrupted via short, sharp pulses that are high in voltage and low in energy. Actually, an output can now be generated via a device about the size of a suitcase, including battery power.

Preventing IEMI

There are many legal requirements and standards for electromagnetic compatibility (EMC) in the industry. The key goal here is to ensure the proper operation of devices in a common electromagnetic environment with regard to any unintentional EMI.

The fact is that just adhering to EMC requirements will not be enough to protect against IEMI. IEMI is generated, via the work of malicious perpetrators, with deliberate attempt to disrupt the proper performance of electronic devices and equipment.



2. Shown are the possible paths for an EMI attack (Image from Reference 12)

Robotic Communication System Immunity from EMI Noise Attack

Designers have created a communications system using a shielded communications hub.[11] This hub interconnects various ports via a controller area network (CAN). The point-to-point communication between each port, along with an interrelated robot device, is established via means of an optical fiber.

This method provides, to the entire system (i.e., the mobile robot), a high level of robustness to EMI *(Fig. 1)*. It offers protection against sabotage by any high-EMI field.

Automotive Analog Integrated Circuitry Under EMI Attack

Modern automotive systems have implemented safety features that help reduce accidents, as well as prevent injuries and fatalities on streets and highways. The marked increase of electronic systems in the automobile has made this possible.

Automotive system designers have strived for robust designs, especially in the areas of safety-critical systems such as anti-lock braking systems (ABS), airbags, electronic stability program (ESP), and more. These systems are designed to meet full functionality, within their specification limits, during any EMI events. EMC is paramount here.

Analog IC Susceptibility to EMI

Integrated circuits, especially analog ICs, have very small dimensions. This makes emission and susceptibility due to conduction more critical than via radiation. It's been found that op amps and other analog blocks, such as voltage references, have a high sensitivity to EMI. These devices are widely used in electronic circuitry designs. However, direct injection of interferences isn't the only path available for EMI *(Fig. 2)*.[12]

One can create a high degree of immunity against EMI by designing a Local Interconnect Network (LIN) integrated output driver circuit. This method can prevent interfering RF signals that may be transmitted via a conductive ground plane, which is common with other analog, digital, or even mixed-signal ICs. Long traces and wires that get routed near a conductive ground plane from the EMI victim will further exacerbate these problems.

The importance of reducing circuit sensitivity, especially when the EMI is directly injected into the input or power-supply pins, must be a top priority. Architectures with higher immunity to the EMI being directly injected into the amplifier input pin will prove to be a far better immunity method, with respect to any EMI interference coupled from the ground plane.

However, it also can be shown that interferences could reach the circuitry from the ground plane by means of capacitive coupling. In this unique scenario, the IC output pin will be a critical point of injection. This mode of susceptibility must be reduced to accomplish solid EMC requirements. The PCB must be designed to help reduce the coupling in this area as well.

Designers may want to add a voltage buffer to the final output stages to reduce any EMI coupled from the ground plane. That's because it can reduce the IC output impedance, which will render EMI coupling less efficient.

Summary

IEMI can generate significant threats—namely, sabotage—in civil, defense, industrial, and commercial sectors, with specific targets such as radio and television, telecom networks, grid power networks, railway networks, air traffic control, and government and banking administrative networks. The susceptibility and vulnerability of these kinds of sensitive systems, caused by EMI both now and in the decades to come, will continue to increase because of the inevitable expansion and spread of radiation sources.

Threats from high-power microwave sources, as well as high-power electromagnetic pulses and high-altitude electromagnetic pulses to civil and defense infrastructure, may include electronic equipment and wireless systems. These may lead to disturbances and damages to electronic devices and wireless systems. Designers must be diligent in their efforts to include methods of recognizing and reducing IEMI into their system designs.

References

1. IEMI – Threat of Intentional Electromagnetic Interference, Martin Ivezic, Cyber-Kinetic Security
2. Intentional Electromagnetic Interference (IEMI), KTH
3. Intentional Electromagnetic Interference (IEMI) – the overlooked threat to IoT, Martin Ivezic, CSO
4. Concerns on the Risk of Malaysian Civil and Defense Systems Due to Intentional Electromagnetic Interference, 2019 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE) 25 - 27 November 2019 at Malacca, Malaysia

5. The Threat of Intentional Electromagnetic Interference (IEMI) – PAN-EUROPEAN TRAINING, RESEARCH AND EDUCATION NETWORK ON ELECTROMAGNETIC RISK MANAGEMENT (etn-peter.eu)
6. Intentional EMI (metatechcorp.com)
7. What Is Electromagnetic Interference (EMI)? How Can You Protect Your Devices Against It? (makeuseof.com)
8. What is Electromagnetic Interference (EMI)? (trentonsystems.com)
9. What is the effect of EMI (Electro Magnetic Interferences) on the human nervous system? (tutorialspoint.com)
10. Tour of the Electromagnetic Spectrum, NASA
11. A mobile robot for vigilance tasks improved with a new robust and low-cost communications system immune to attacks with EMI noise, 2005
12. Analog ICs for Automotive under EMI Attack, Department of Information Engineering University of Brescia, 2019

Captions: