Wireless Digital Security for Industry 4.0

HARMONY IoT
BY ORCHESTRA GROUP

Executive Summary

Flexible, flawless, large scale machine- to- machine (M2M) communication is critical for Industry 4.0 and smart factories to succeed and is driving the adoption of wireless communication technologies like Zigbee, Bluetooth, LoRa, and Wi-Fi. Wireless connectivity breaks down walls and barriers, making it simple and flexible to use, but opens up factories to a unique set of cyber risks that can lead to **manufacturing disruptions, data theft, and ransomware**. Physical security controls, such as guards and gated entries protect your wired devices and networks, but do not prevent an attacker from using wireless from a public area to gain unauthorized access or disrupt production.

Harmony IoT is the only airspace protection solution that prevents and protects against airspace attacks, mitigates ongoing attacks, and provides the information needed to enable your physical security team to quickly locate the source of the airspace disruption – and can save lots of money in production down time.

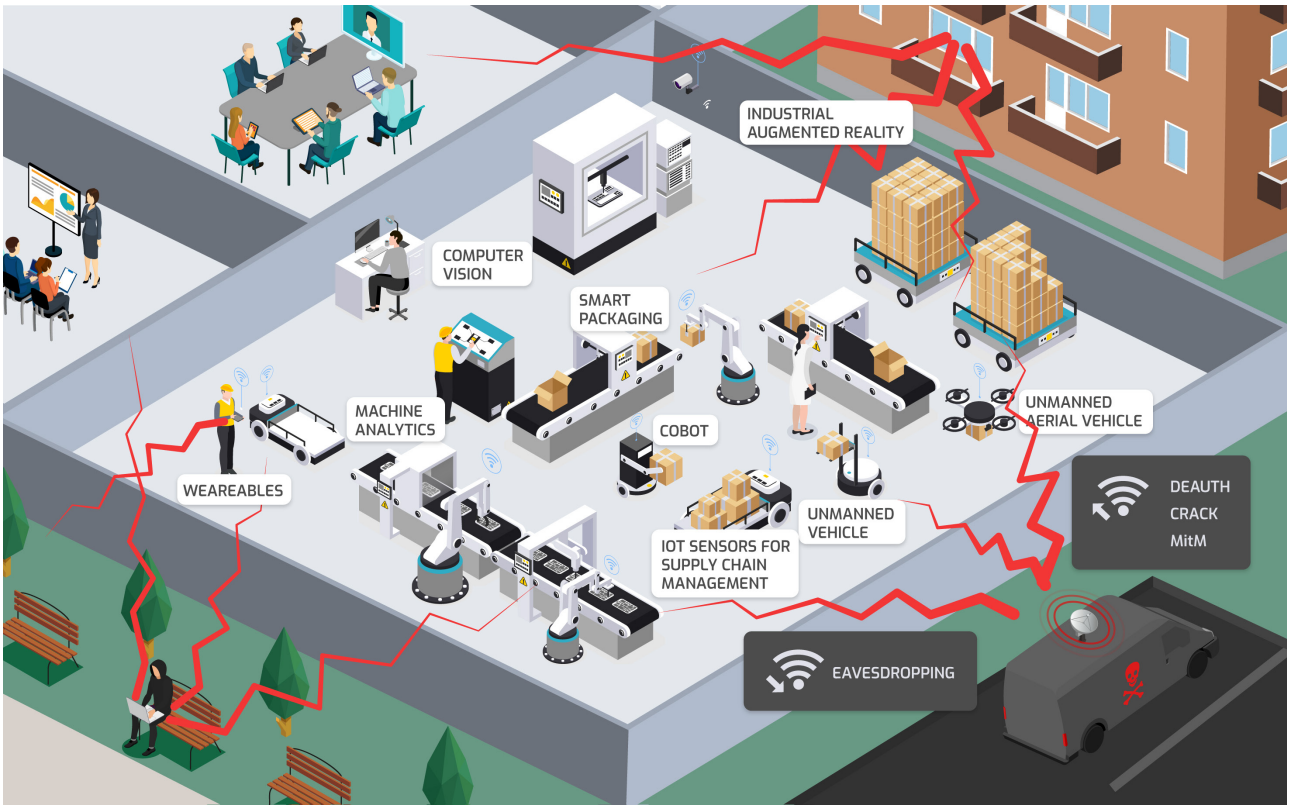

Figure 1: WiFi breaks the virtual walls

Wireless as an Attack Vector

All that is needed to attack a wireless network from a bench, a van located outside your premises, or from an office kilometer away, is a $200 attack device easily concealed in a backpack. Attacks like Karma, Evil Twin, or Wireless Deauth can be highly effective in disrupting manufacturing processes and even short disruptions can cost a lot of money.

Wireless enables attackers to scout your devices and monitor your processes invisibly without breaching your existing physical or web security. Wireless attackers use "off the shelf" toolkits and devices to scout and attack the airspace, and no special skills are required. In addition, internal airspace risks need to be managed in order to protect against employee error that can be caused by their mobile phone's hotspot These disruptions can directly cost a lot of money in lost production.

Wireless Process Risk

For Industry 4.0, process risk is very tangible and quantifiable – it is the production cost of unexpected down time. A wireless process attack targeting your airspace can easily disrupt proper factory operations by disconnecting a critical piece of equipment from its access point, or from another production step.

Harmony IoT can differentiate between an attack and a wireless glitch and provide your security team with the location of a rogue device.

Maintaining Wireless Cyber Hygiene

The first step in managing airspace cyber risk is to ensure "wireless cyber hygiene" proactively preventing and protecting against known wireless threats.

Harmony IoT monitors the basic health and security of your wireless networks and equipment, provides the cyber hygiene needed against wireless threats such as Karma, Evil Twin, or Wireless Deauth. **Harmony IoT** cyber hygiene also provides a buffer against unknown threats that depend on a weakness like unpatched or misconfigured systems.

Automating Wireless Attack Response

The next step is to quickly detect and respond to wireless attacks in your airspace.

Harmony IoT enables automated response and enforcement of wireless policies to protect your airspace. For example, Harmony IoT can enforce a policy to "restore the walls" and make your wireless airspace risk profile on par with your wired network.

Summary: Harmony IoT Protects the Factory Airspace

As factories become "smarter" and more dependent on the CIA (confidentiality, integrity, and availability) of their airspace, – there needs to be controls in place to protect against this growing attack vector. **Harmony IoT** is the only out- of- band solution that monitors, predicts, and protects your factory airspace against wireless attacks.

Harmony IoT protection can be provided through a cloud service, or as an on-premises solution. Because it is out-of-band, **Harmony IoT** is simple to set up as a proof of concept and generates no new risks to your existing network protections.

Who

A large Global manufacturer uses an online wireless inventory management system to continuously monitor and optimize production line inventory. The system is critical for correct operation of the production line, and if the system is not performing adequately production can grind to a complete halt – at a cost of 10,000 euros per minute.

Wireless Hygiene

No "Hot-spots" are allowed on the manufacturing floor due operational disruption concerns that might result from overcrowding the equipment airspace. Before **Harmony IoT**, the customer had no practical way to monitor and enforce this policy. Harmony IoT provided visibility into "Hot-spots" which immediately reduced the number of "Hot-spots" by 70%, even before applying proactive mitigation enforcing the corporate policy.

Wireless risk policies

Only on-premise devices are permitted to access networks in a sensitive production area and from specific location. An allowed device outside of the area are mitigated, as are all other external devices. Harmony IoT enforces the policy by mitigating external devices (known and unknown) from connecting to internal networks. This radically lowers the risk of wireless operational disruptions, production line failures and ongoing loses.

Contact us today to arrange for a demo or proof of concept.

info@orchestragroup.com