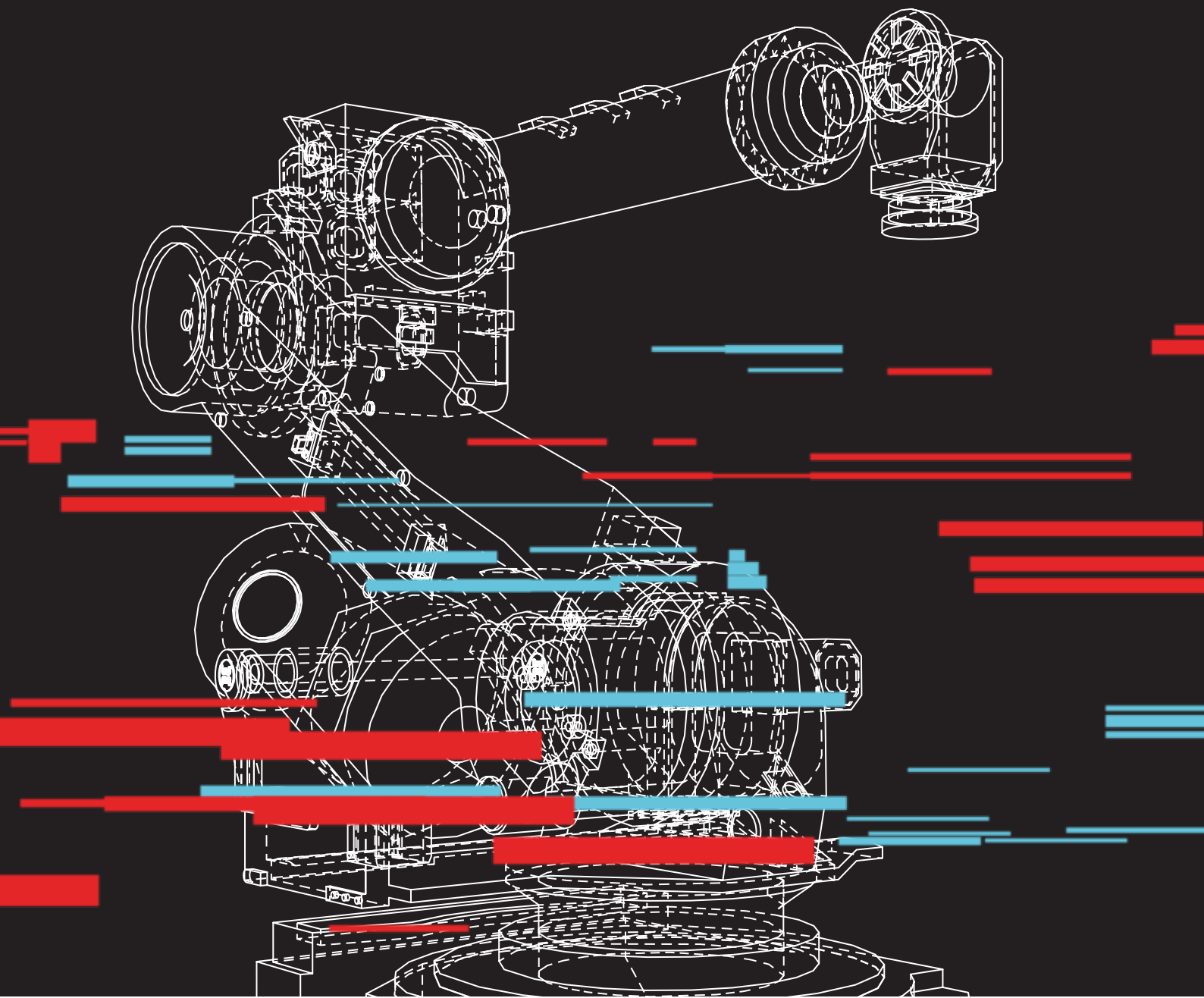
HARMONY IoT
BY ORCHESTRA GROUP

Wireless Digital Security for Industry 4.0

July 2021



Protecting Smart Factory
Executive Summary

As manufacturing moves into the digital era, factories are becoming smarter by using digital technologies to continuously collect and share data through connected machines, devices, and production systems. This improves manufacturing processes and the ability to respond to new demands and changing markets.

These cyber-physical systems form the basis of Industry 4.0 (for example, "smart machines"). They rely heavily on information and communication technologies, enabling new ways of production, value creation, and real-time optimization. Cyber-physical systems create the capabilities needed for smart factories and is the driving force behind IT-OT convergence.

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. The dark side of these technologies is that they open up factories to a new world of cyber airspace risk. Cyber attack techniques that used to be only in the realm of IT have now jumped the fence to OT, and are being used not just to steal data, but also to disrupt manufacturing processes. No organization would knowingly open their production directly to the internet for fear of a cyber attack, but many routinely leave their airspace unprotected. Wireless connectivity opens up factories to a unique set of cyber risks that can lead to manufacturing disruptions and data theft. Smart factories must deploy controls to protect their airspace from cyber attack, just as they protect against traditional cyber attacks.

Wireless connectivity breaks down walls and barriers, making it simple and flexible to use. Wireless connectivity does not demand physical, fixed connection points or "ports." Wireless devices connect invisibly through the airspace access points and from there to the rest of the network. This flexibility and reach is the also the Achilles heel of wireless, making them easier to attack and compromise from public areas. Physical security controls, such as guards and gated entries, protect your wired networks, but do not prevent an attacker from using your wireless networks to gain unauthorized access or disrupt production. All that is needed to attack a wireless network from a bench, a van located outside your premises, or an office kilometers away, is a $200 unit 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 tens of thousands of euros.

Harmony IoT is an out-of-band solution that protects your airspace by creating a wireless dome of protective policies for wireless connectivity and access. It protects manufacturing processes from airspace attacks and disruptions, but it doesn't have to be directly connected to your network in order to provide airspace protection.

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 airspace disruption so that it can be handled directly.

Data Breaches by Sectors

444% rise in Manufacturing Sector, 88 in Finance

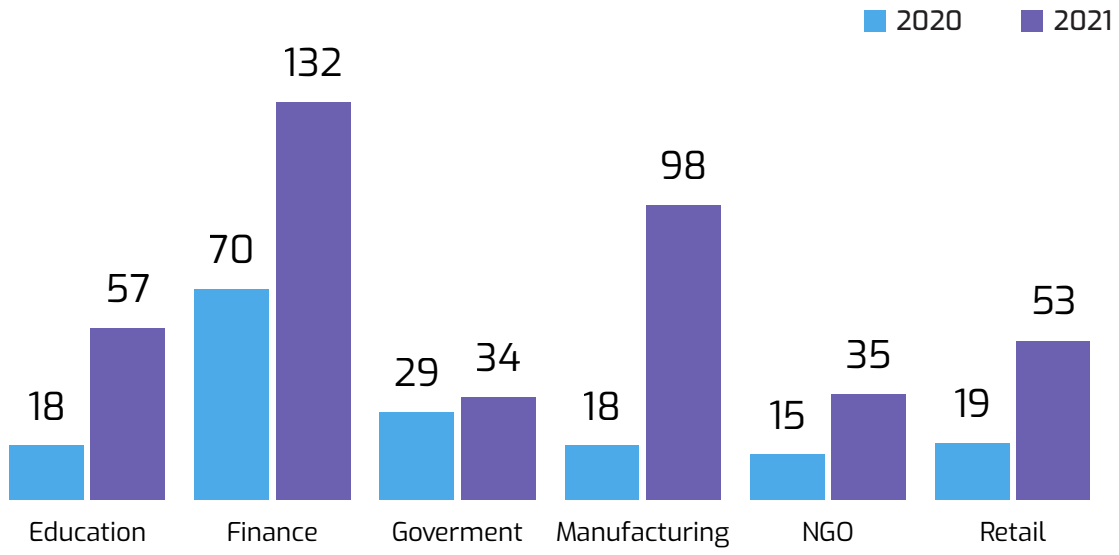


Figure 1: Number of Breaches reported in six months to the first of July each year. Published July 2021.
* UK Manufacturers Organization (EEF)

Wireless as an Attack Vector

Unlike wired connectivity, wireless connectivity is not constrained by the physical boundaries of a factory – wireless signals penetrate windows, doors, and walls. Wireless signals are visible to attackers from over a kilometer away for Wi-Fi, and 10 kilometers for LoRa. Wireless enables attackers to scout invisibly and without breaching your existing physical or web security. The US Cybersecurity and Infrastructure Agency (CISA) has actually recommended that home networks reduce wireless signal strength to lower the risk of wireless attack. This recommendation is impractical in an industrial setting (since lowering power can cause disconnects) and a motivated attacker can still intercept a signal that has limited coverage.

Wireless attacks are no longer the purview of highly sophisticated attackers that develop their own tools. Wireless attackers now use "off the shelf" toolkits and devices to scout and attack the airspace. On the other hand, organizations have very few choices when it comes to protecting their airspace. Not protecting your airspace is the equivalent of putting a wired LAN port on the sidewalk outside your building so that anyone can connect and "try their luck." Every CISO knows that even with the best internal defenses, given enough time and effort, any defense can be breached. Ignoring wireless risk is an attack waiting to happen.

Internal airspace risks need to be managed as well – no matter whether they are driven by bad actors in the organization, or just by employee error. In today's world every employee carries a powerful access point in their pocket (also known as a mobile phone) that can maliciously or inadvertently disrupt factory connectivity. No matter what the cause of the disruption, the result is the same – factory downtime and thousands of euros in lost production.

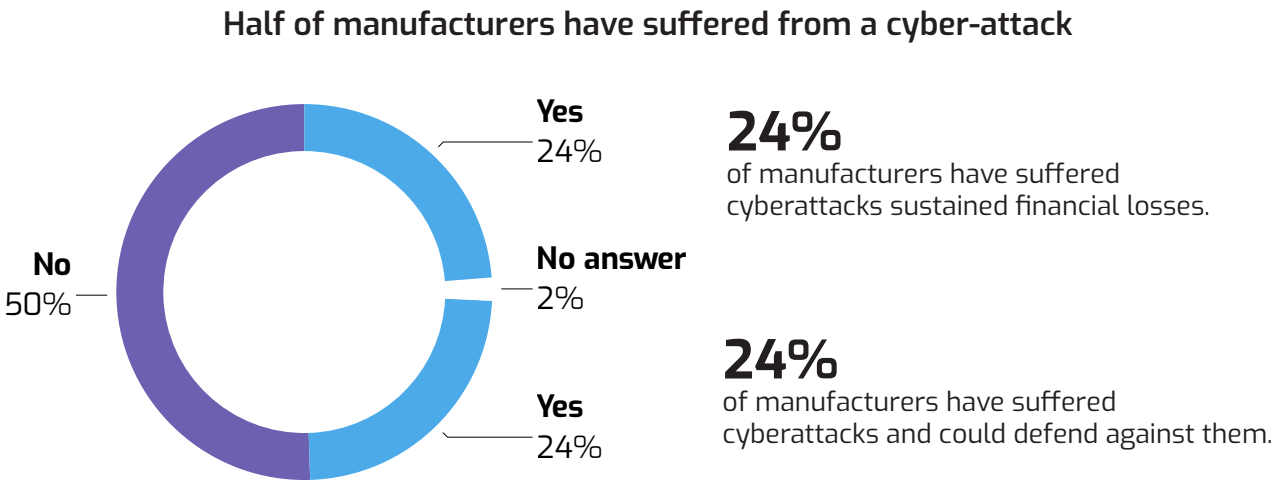


Figure 2: manufacturers cyber-attacks statistics
* UK Manufacturers Organization (EEF)

Process Risk vs Data Risk

Most M2M data doesn't contain sensitive information, which leads some organizations to ignore the risk of wireless communication, thinking the worst-case scenario is a loss of some "unimportant data." Nothing could be further from the truth since the real danger in wireless attacks is process disruption, or as a stepping stone to a general network breach. Cyber attackers don't start directly with the object of the attack. They search for the weakest link and advance to an "interesting" target. Industry 4.0 smart factories have made the wireless airspace the weakest link.

For industry, process risk is very tangible and quantifiable. It is the production cost of unexpected downtime. A process attack targeting your airspace can easily disrupt proper factory operations by disrupting devices or access points on the factory floor. Without appropriate wireless cyber controls, these attacks can be very difficult to detect and mitigate. Take the simple scenario of an attacker disrupting connectivity between a critical piece of equipment and its access point, or to another production step. This type of attack is difficult to detect since specific controls are needed to differentiate between an actual attack, or just a short-term network glitch. Finding the attacking device can be even harder. The cost of such a disruption can range between hundreds or thousands of euros per minute. Every minute the attack is not identified and addressed directly results in fewer products delivered.

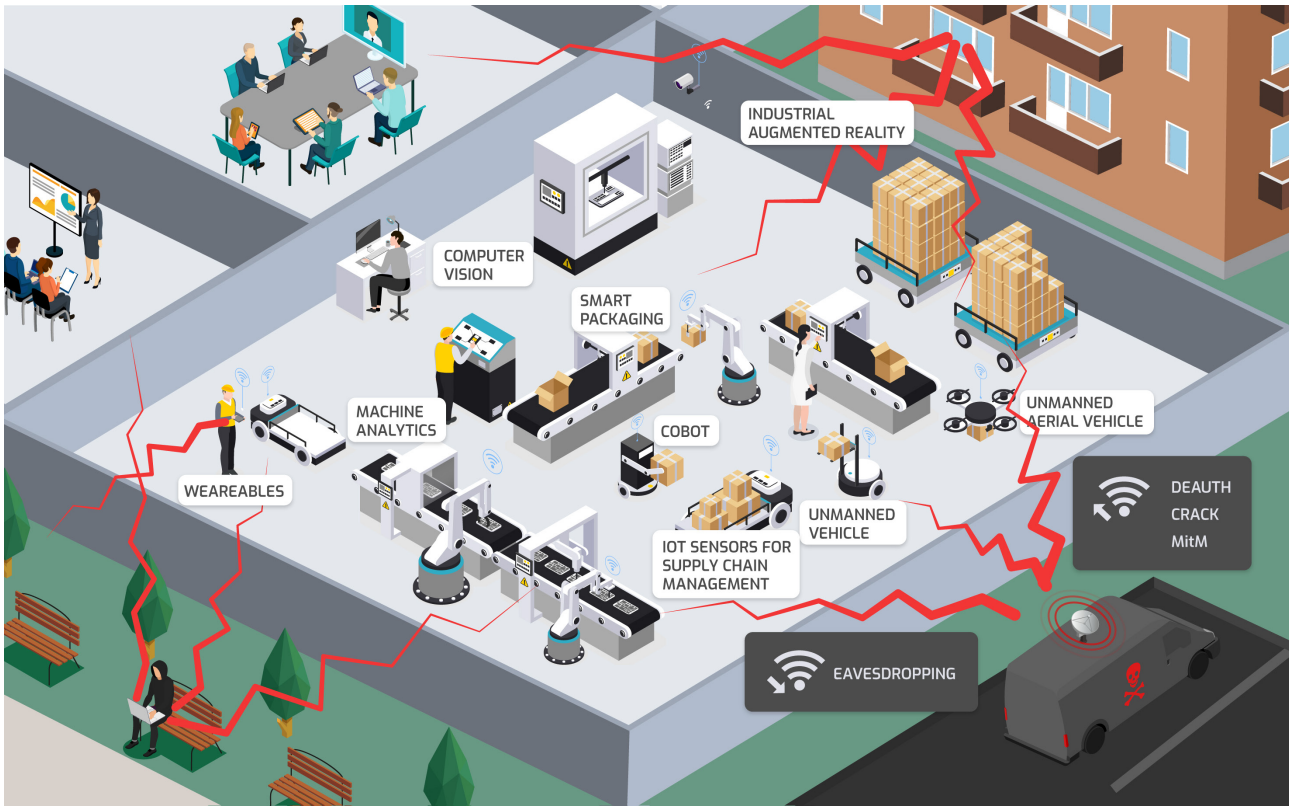


Figure 3: WiFi breaks the virtual walls

Another type of airspace attack is to create an “evil twin” or other type of rogue access point. In this type of attack the target is the factory network itself. Once equipment has connected to the rogue access point, an attacker can attack the device itself and use it as a bridge to the factory network or to keep it from working properly in production. Once inside the factory network, attackers can do as they please. This includes stealing or encrypting sensitive data as part of a ransomware attack or performing a process attack to disrupt production processes either for “fun” or ransom.

Wireless Hygiene Minimizes Wireless Attack Risks

So what can be done? A risk-based approach is the best way to manage wireless threats. That entails understanding airspace risks posed by wireless communication and deploying operational controls such as **Harmony IoT** to manage wireless risk in accordance with the organization’s risk appetite.

The first step in managing airspace cyber risk is to ensure “wireless cyber hygiene” by monitoring and maintaining the basic health and security of your wireless networks and equipment. Wireless cyber hygiene is the basis for proactively preventing and protecting against known threats such as Karma, Evil Twin, or Wireless Deauth. Wireless cyber hygiene also provides a buffer against unknown threats that depend on a weakness like unpatched or misconfigured systems. **Harmony IoT** continuously monitors your wireless cyber hygiene:

Monitors the confidentiality of the corporate airspace.

- Monitor SSID encryption levels.
- Monitor WLAN (Wireless LAN) connected device separation.

Monitors the integrity of the corporate airspace.

- Monitors the integrity of corporate SSIDs, APs, and hotspots accessible in the corporate airspace.
- Monitors the integrity of the access path between a connected device and its associated AP.
- Monitors the WLAN device separation.
- Monitors any relation between corporate airspace and general airspace outside.

Automating Wireless Attack Response

Wireless cyber hygiene is the first step in minimizing wireless cyber risk, but no matter how good your wireless cyber posture, you still need 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 risk profile:

- Disconnect wireless equipment in the corporate airspace associated with unknown APs.
- Disconnect wireless equipment in the corporate airspace associated with APs outside the corporate airspace.
- Disconnect wireless equipment outside the corporate airspace associated with any AP in the corporate airspace.
- Disconnect any devices connected to a hotspot.

As well as enforcing policies, **Harmony IoT** continuously scans your airspace looking for indicators of an active attack and automatically disconnects devices or provides your security team with a location notification so that they can physically find and remove the source of the attack. The decision is based on attack severity and your risk appetite as described in your policies.

For example, an attacker may try to create an "evil twin" and attempt to get devices to connect to their access point instead of a corporate access point. This attack would be recognized by **Harmony IoT** and it would respond to the ongoing attack by wirelessly disallowing any connections to the rogue hotspot. **Harmony IoT** will also notify you of the attack's location so that your security team can have it physically removed.

Summary

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

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.

On a specific day the system began to “hiccup” – slowing production. Since **Harmony IoT** was installed the month before, it was already monitoring and collecting information from the airspace. No attacks or unusual incidents were observed, so then **Harmony IoT** was used to analyze other parameters of the wireless network (both current and historical).
The culprit was found, the issue located and corrected.

The same customer has two proactive wireless risk management policies:

- 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.

- 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.