Protecting the Smart Factory

Date: May 2021

Copyright

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Protecting the Smart Factory

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.

Many smart factories utilize wireless communication technology to provide the flexible device and network connectivity needed. Wireless connectivity is proven, ubiquitous, and flexible. It also opens up factories to an entirely new set of cyber risks that can lead to manufacturing disruptions.

Wireless connectivity's benefit is that it breaks down connectivity walls and barriers. Unlike wired networks, it does not require physical, fixed connection points or "ports." The liability is that wireless networks are much easier to attack and compromise because they are visible and accessible from public areas. Physical security controls, such as guards and gated entries, do not prevent an attacker from attempting to eavesdrop on wireless communications or gain unauthorized access to internal or wired networks.

All that is needed to attack your wireless networks from a bench or van located outside your premises is a $200 unit that is easily concealed in a backpack. Attacks like Karma, Evil Twin, or Wireless Deauth can be highly effective in disrupting your manufacturing processes.

Harmony-IoT is a proven solution that creates a wireless dome of protective policies for your airspace. It builds walls around your networks and protects your manufacturing processes from airspace attacks and disruptions.