Hello there,

As we close out another successful year and look to the future, three dominant drivers remain in effect: the need to protect devices that are increasingly interconnected; the fact that increasingly connected operational technology (OT) has unique and increased security needs; and the certainty that meeting those unique needs requires built-in cyber security. This month we highlight articles that show that the cyber security services industry is moving in this direction as well.

And as 2019 ends, I would also like to thank you for your interest in open secure automation and for your continued support and interest in Bedrock solutions. I wish you all the best in the new year and look forward to continued communication.

May your holiday season be filled with peace and joy,

Albert Rooyakkers
Founder, CEO
Bedrock Automation

State of Industrial Cyber Security 2019

Although industrial enterprises are becoming increasingly aware of the cyber security challenges of digital transformation, they are not necessarily applying cyber security best practices regularly. This is among the many findings in a report from a Netherlands-based engineering firm that specializes in OT cyber security.

Read more.
IoT Cyber Security Predictions for 2020

IoT implementations are expanding steadily and with them concerns for cyber protection. See what some cyber security service specialists believe will be top of mind for IoT security in 2020.

Read more.

Extracting Value from Smart Infrastructure

It's no coincidence that interest in securing OT and interest in embedded cyber security are advancing hand in hand. More and more companies are recognizing that the most economical and effective way to secure operational technologies such as control systems and field devices is by embedding authentication and encryption capabilities in at the design phase.

Read more.

“New smart infrastructure promises connectivity wins but cybersecurity risks.”

Dr. Rida Hamza
VP, Critical Infrastructure Protection at Parsons