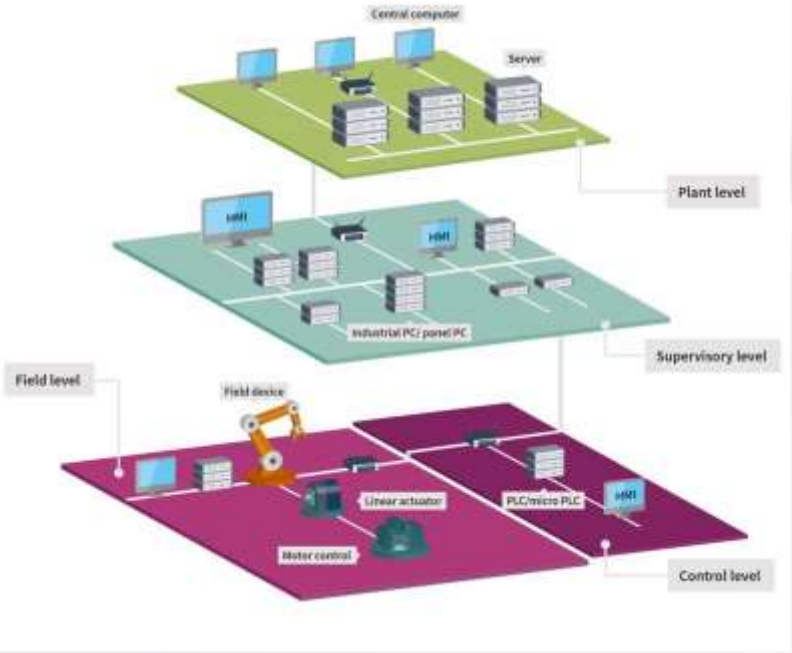
STANDARDS FOR SECURING INDUSTRIAL EQUIPMENT

Along with the promise of more capable products and systems resulting from the Internet of Things (IoT), there are also increased security risks. While any organization should already be aware of and reacting to these security threats, users of industrial automation should be more concerned and prepared than most. Otherwise, they may end up with major equipment damage as recently happened in German steel mill.[1]

In smart factories, also known as the Industrial Internet of Things (IIoT) or Industry 4.0, the shop floor is no longer separated from the rest of the world. Instead, the industrial plant is highly connected, both to receive customer orders from outside and to send back data for analysis. Opening up the factory floor means that hackers can get in, even at the lowest levels. As a result, security risks touch everything in the factory now. And the IIoT extends beyond factories to oil, gas, chemicals, logistics and transport, and many other areas where industrial controls are used. So this domain is quite broad.

The Trusted Computing Group (TCG) and other organizations are making targeted efforts to improve security for industrial equipment, whether connected or not. TCG already has developed a number of specifications and documents to help address industrial security, including:

- TCG IoT Architect's Guide (http://bit.ly/1RzLRa6)
- TCG Guidance for Securing IoT (http://bit.ly/2f8RYkK)
- TNC IF-MAP Metadata for ICS Security https://trustedcomputinggroup.org/tnc-if-map-metadata-ics-security/
- Architects Guide: ICS Security Using TNC Technology https://trustedcomputinggroup.org/architects-guide-ics-security-using-tnc-technology/



More recently, TCG has worked with the Industrial Internet Consortium (IIC) on its Industrial Internet Security Framework (https://www.iiconsortium.org/IISF.htm). In fact, the Industrial Internet Security Framework specifically references TPM as a recommended technology for securing endpoints.

Another major standard for industrial security is IEC/ISA 62443, an international standard in this area. IEC/ISA

[1] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Copyright © TCG 2017

62443 is actually a series of documents not just one document. IEC 62443-4-2 (Technical security requirements for IACS components) mentions TPM and requires that hardware security must be used to protect authenticators like cryptographic keys, at least for the two highest security levels.

With a goal of more fully applying Trusted Computing techniques to secure industrial equipment, TCG in 2017 has created a new Industrial Sub Group in the Embedded Systems Work Group. To make this effort successful, experienced, interested stakeholders should **join TCG and join the Industrial Sub Group** (https://trustedcomputinggroup.org/membership). Those interested in industrial security, should be integrally involved when the standards are being defined. The first identified deliverables are:

- TCG Guidance for Securing Industrial Equipment
- TCG TPM 2.0 Platform Firmware Profile for Industrial Equipment

For more information, email: admin@trustedcomputinggroup.org

Copyright © TCG 2017