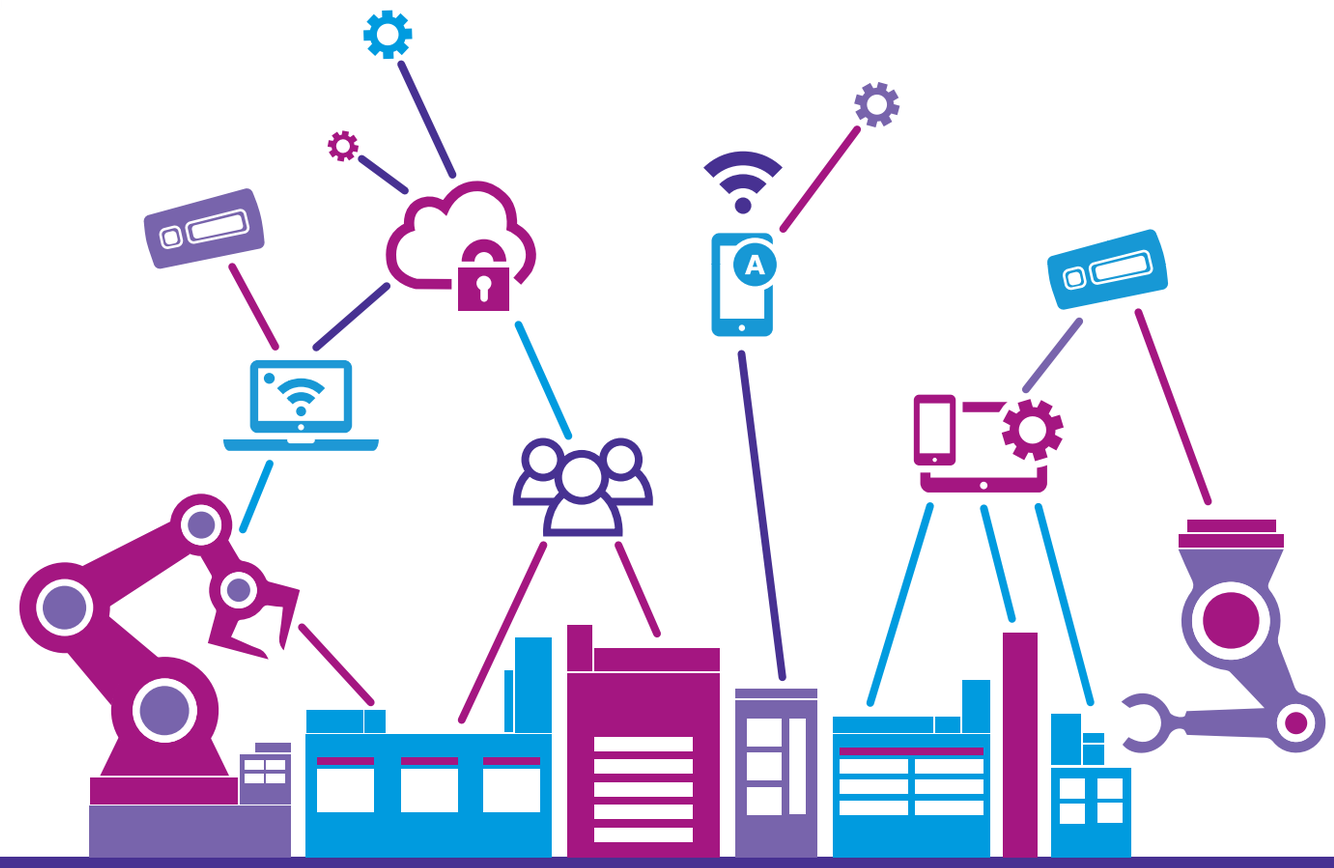
The rise of smart factories and the cybersecurity risk they pose

The rise of smart factories will help the manufacturing industry considerably, as digital technology such as automation can lead to greater efficiency and accurate reproducibility, leading to optimum product quality with minimum waste.

But, these connected devices expose a greater risk for hackers to remotely attack all aspects of the supply chain. As these threats increase, manufacturers need to ensure they are protecting their systems in the correct way to minimise unauthorised access.



The future of the factory

Digital transformation trends in manufacturing

IoT & Industry 4.0

AI & machine learning

Robots

Improved efficiency

Data and analytics

Smart factory adoption per industry by 2020:

Electronics

Industrial manufacturing

Aerospace

Engineering & Construction

Automotive

The risks...

of manufacturers have been subject to a cyber-attack

said 'yes, we have sustained financial or other business losses'

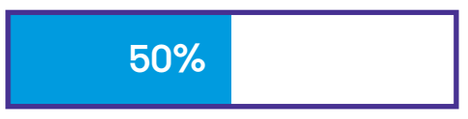
of manufacturers are investing in digital technology

consider cyber vulnerabilities inhibit them from doing so fully

of cyber-attacks will target Internet of Things devices by 2020

of manufacturers have invested in cyber security training

do not have any technical support in place to assess cyber-attacks



are reviewing their cyber-security due to GDPR

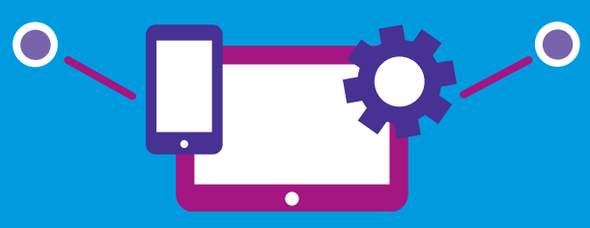
Risk management

MFA

can be used to protect applications such as ERP systems and to protect your CRM

Jump host

can be protected with MFA onto the control network



This will separate MES from PLM and ERP

ISO 27000

series of security standards have been issued to help businesses manage their data assets

Sources:

Information Age. 2018. The Internet of Things: The security crisis of 2018. [ONLINE] Available at: https://www.information-age.com/internet-things-security-crisis-123470475/

Moschip. 2018. Smart Factories Infographic. [ONLINE] Available at: https://moschip.com/wp-content/uploads/2018/05/Smart-Factories-infographics-final-1.jpg

EEF. 2018. Cyber Security for Manufacturing. [ONLINE] Available at: https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cyber-security-for-manufacturers

Forbes. 2017. Top 5 Digital Transformation Trends in Manufacturing. [ONLINE] Available at: https://www.forbes.com/sites/danielnewman/2017/08/08/top-5-digital-transformation-trends-in-manufacturing

Abbreviation Glossary:

MFA: Multi-factor authentication - a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login.

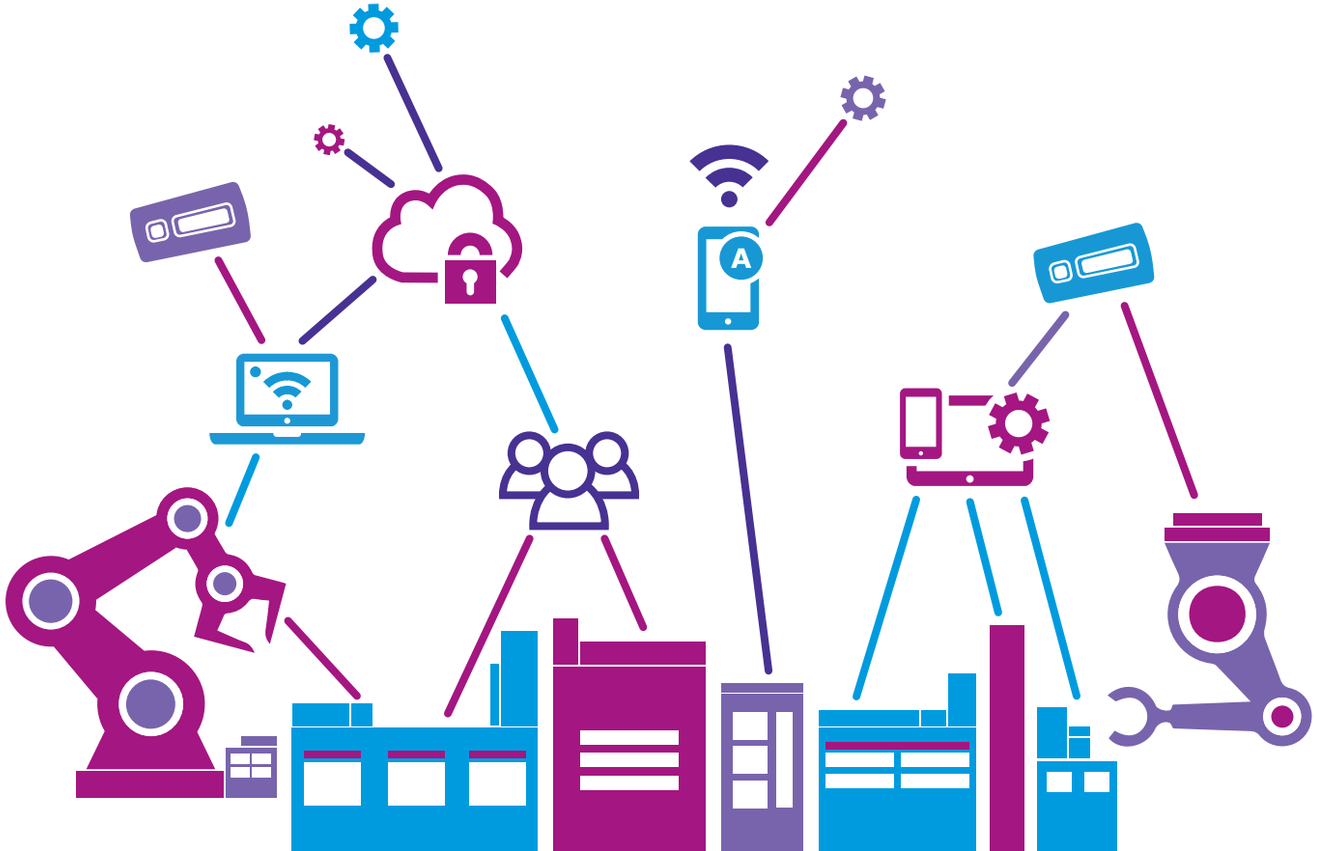
ERP: Enterprise resource planning

MES: Manufacturing execution system

PLM: Product lifecycle management

swivelsecure

www.swivelsecure.com



The future of the factory

Digital transformation trends in manufacturing

IoT & Industry 4.0

AI & machine learning

Robots

Improved efficiency

Data and analytics

Smart factory adoption per industry by 2020:

Electronics

Industrial manufacturing

Aerospace

Engineering & Construction

Automotive

Risk management

MFA

can be used to protect applications such as ERP systems and to protect your CRM

Jump host

can be protected with MFA onto the control network

This will separate MES from PLM and ERP

ISO 27000

series of security standards have been issued to help businesses manage their data assets

The risks...

of manufacturers have been subject to a cyber-attack

said ‘yes, we have sustained financial or other business losses’

of manufacturers are investing in digital technology

consider cyber vulnerabilities inhibit them from doing so fully

of cyber-attacks will target Internet of Things devices by 2020

of manufacturers have invested in cyber security training

do not have any technical support in place to assess cyber-attacks

are reviewing their cyber-security due to GDPR