Naz Khaleque

November 2019

RESILIENT INDUSTRIAL NETWORKS

Preparing for Tomorrow's Connectivity

Honeywell

Agenda

Today's process control environments rely on traditional **connectivity technologies and protocols**, but how are these vulnerable to potential cyber-attacks, how can the risks be mitigated, and what are the technologies of tomorrow that operators can start planning for?

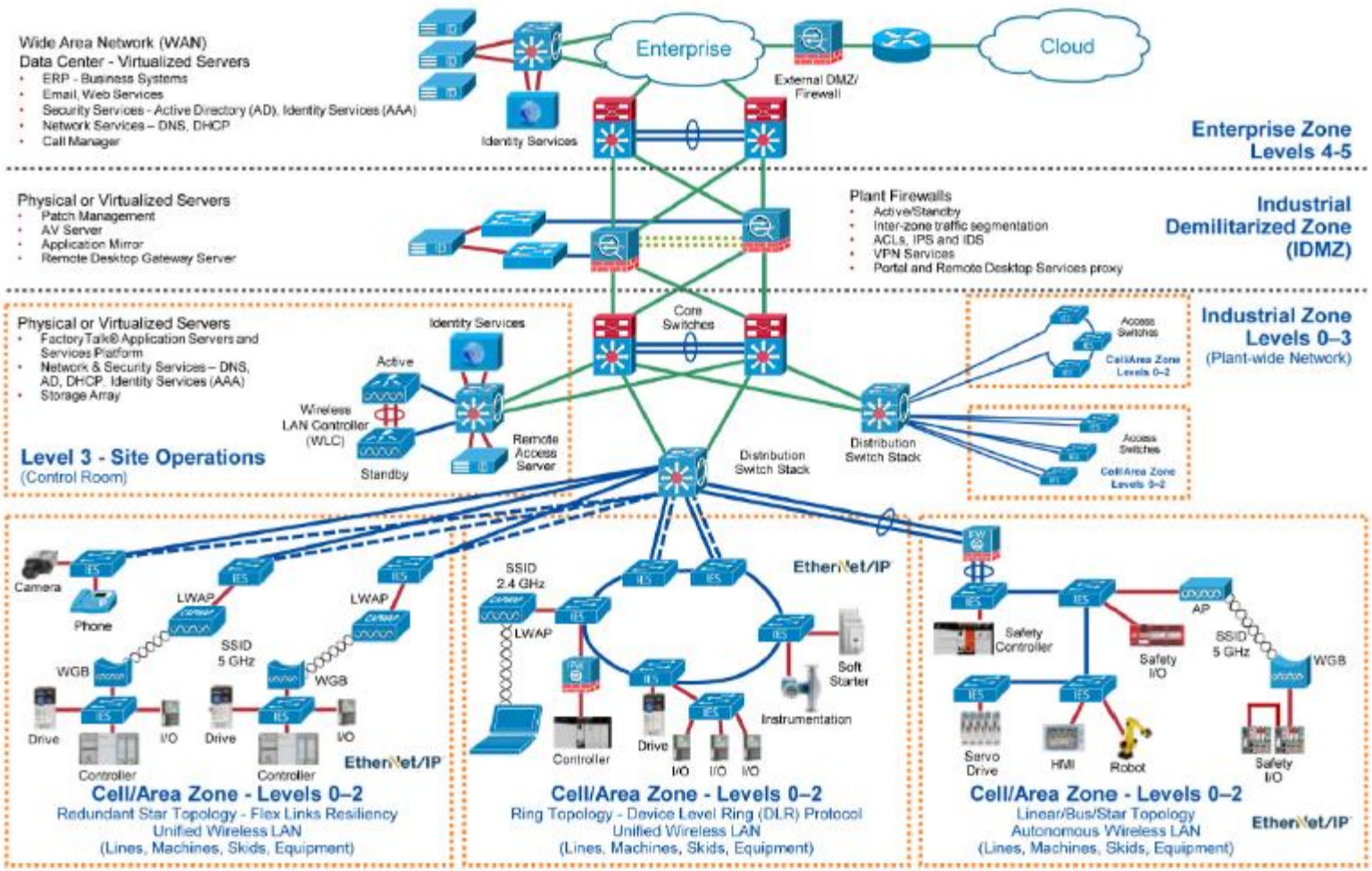
- Converged Plantwide Ethernet Architecture (CPwE)
- Cybersecurity - OT Misconceptions
- Top 10 Threats 2019
- Commonly Used Tools
- Uni-directional and Bi-directional Communications
- ICS Protocols
- EtherNet/IP + CIP
- Edge Device Security
- 5G for Connected Industries and Automation
- 5G Expands Cyber risk
- Hacking Industrial Control Systems
- Summary: High-level Challenges on Communications
- Final Word

Honeywell

Converged Plantwide Ethernet Architecture (CPwE)

A holistic resilient plant-wide network architecture is made up of multiple technologies (logical and physical) deployed at different levels within the plant-wide architecture:

- Robust physical infrastructure
- Topologies and protocols
- Switching and routing
- Wireless LAN Controllers (WLC)
- Firewalls
- Network and device management



Source: Rockwell Collins & Cisco -Document Reference Number: ENET-TD010B-EN-P

Honeywell

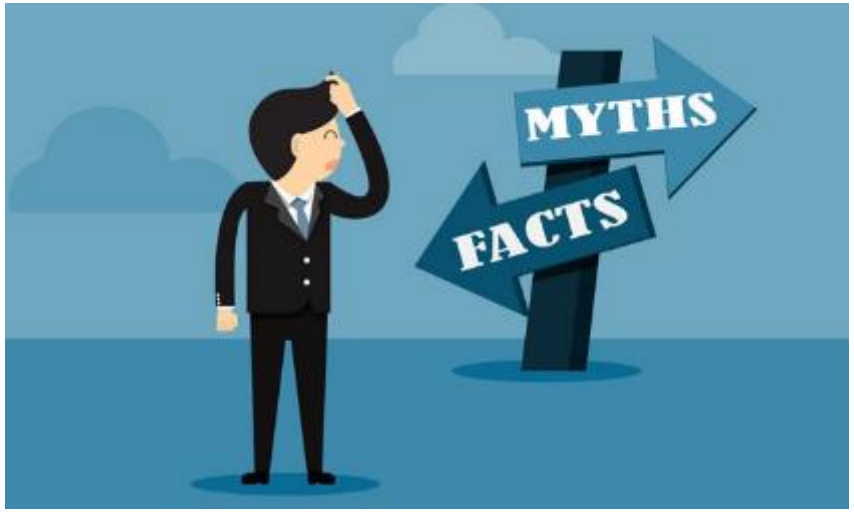
Cybersecurity - OT Misconceptions [1]

A. Denial of Reality

B. Misplaced Trust in Security Technologies

C. Incorrect Assumptions About Technological

D. Reductive Views on Security



1. **Industrial Control Systems (ICSs) are Isolated**

   The average Industrial Control System (ICS) has 11 direct connections [2]

2. Nobody Wants to Attack Us

3. **We Only Have Obscure Protocols/systems**

   SCADA and process control systems are common topics at hacker's "Blackhat" conferences [2]

4. Anti-Virus and Patching are Useless for ICSs

5. Cybersecurity Incidents Will Not Impact Operations

6. Social Engineering is not an ICS Issue

Source: *[1] Ludovic Piètre-Cambacédès, Member, IEEE, Marc Tritschler, and Göran N. Ericsson, Senior Member, IEEE*
[2] Kaspersky Lab

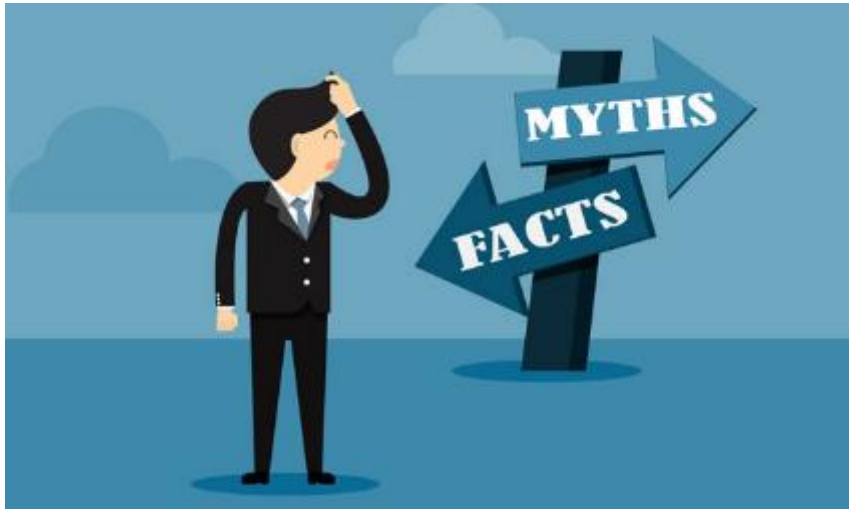
Cybersecurity - OT Misconceptions [1]

A. Denial of Reality

B. Misplaced Trust in Security Technologies

C. Incorrect Assumptions About Technological

D. Reductive Views on Security



1. Our Firewall Protects us Automatically

Almost 80 per cent allowed "Any" services on inbound rules as well as unsecured access to the firewalls and demilitarized zone [2]

2. One-Way Communication Offers 100% Protection

The nature and strength of the protection provided by each enforcement policy differs to a great extent.

1. It's Encrypted: It's Protected

2. Anti-Virus Protection is Sufficient

Source: *[1] Ludovic Pietre-Cambacédès, Member, IEEE, Marc Tritschler, and Göran N. Ericsson, Senior Member, IEEE*
[2] Kaspersky Lab

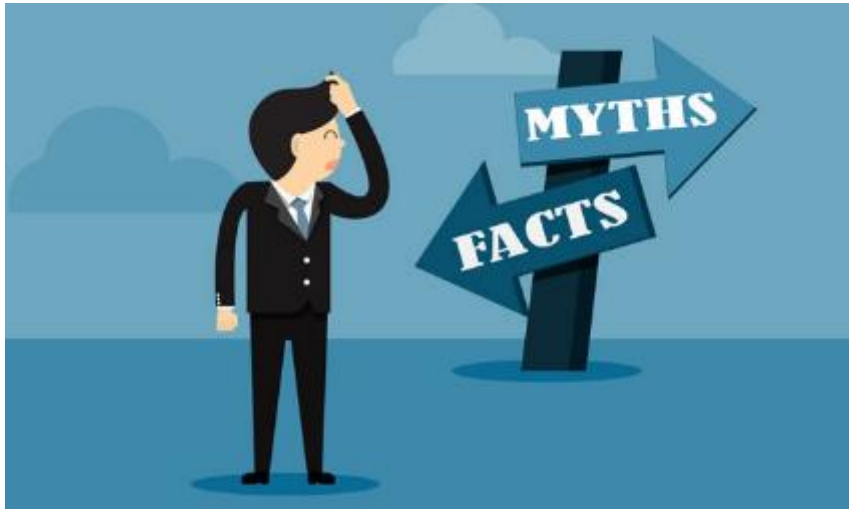
Cybersecurity - OT Misconceptions [1]

A. Denial of Reality

B. Misplaced Trust in Security Technologies

C. Incorrect Assumptions About Technological

D. Reductive Views on Security



1. **Obscure Protocols/Systems are Naturally Secure**

   even that which seems to be extremely specific or "obscure" is often, in fact, openly documented.

2. **Serial-Link/4–20 mA Wire Communications are Immune**

   Serial links are digital channels, and like TCP/IP, they make no distinction between malicious and non-malicious traffic that they carry.

3. ICS Components do not Need to be Security Hardened
4. ICS Security is a Technological Problem
5. It's Certified, It's Secured
6. Vendors Have a Full Command of Their Products Security
7. Compliance With Security Standards Makes You Secure
8. ICS Security Assessment Does not Need Full Inventories
9. Access Points to ICSs are Easily Controlled
10. Security is a Problem that Needs to be Solved Only Once
11. Cybersecurity can be Handled at the End of the Project

Source: [1] *Ludovic Piètre-Cambacédès, Member, IEEE, Marc Tritschler, and Göran N. Ericsson, Senior Member, IEEE*

Top 10 Threats 2019

Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	→
Intrusion via Remote Access	→
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	→

Source: 2019 BSI Publications on Cyber-Security

Honeywell

Commonly Used Tools

The Rubber Ducky is a memory stick lookalike which is not a memory stick but a device which replicates the keystrokes of a keyboard.

The Bash Bunny by Hak5 is the world's most advanced USB attack platform. It delivers penetration testing attacks and IT automation tasks in seconds by emulating combinations of trusted USB devices – like gigabit Ethernet, serial, flash storage and keyboards.

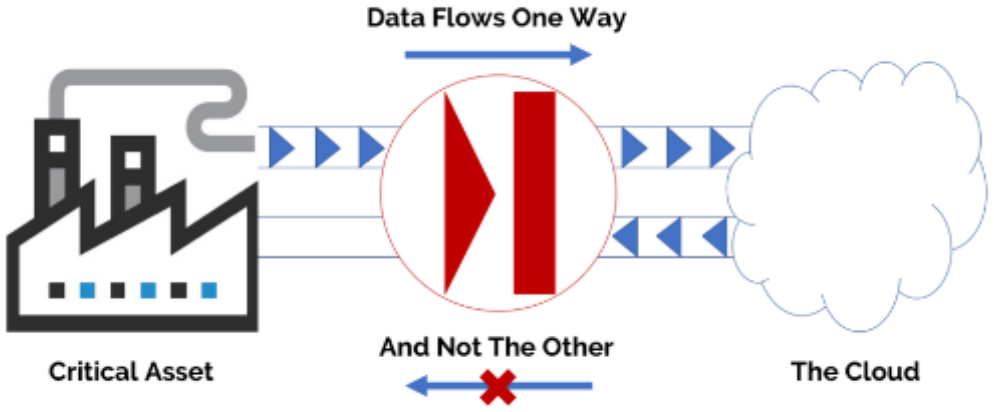
Top 10 Threats 2019

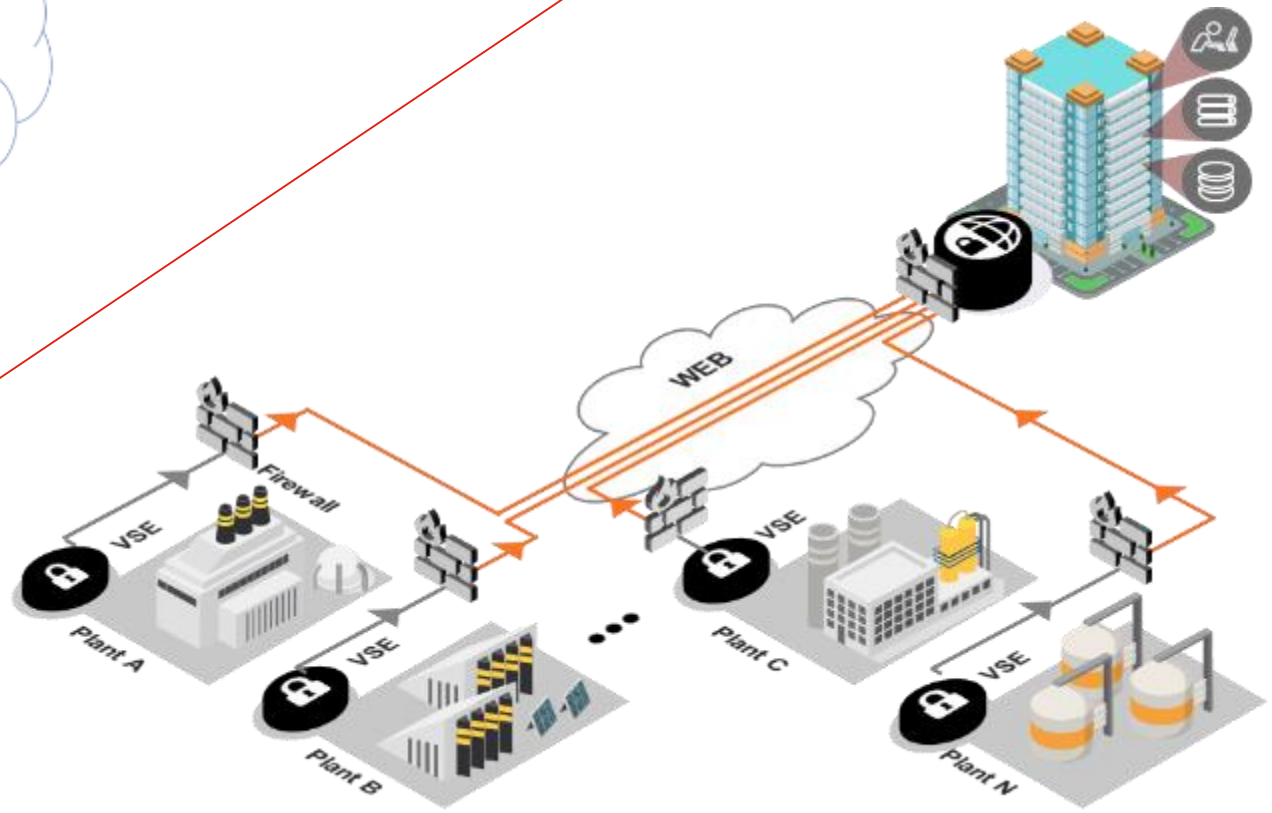
Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	→
Intrusion via Remote Access	→
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	→

Source: 2019 BSI Publications on Cyber-Security

Honeywell

Uni-directional and Bi-directional Communications





Honeywell

ICS Protocols

Standard OT protocols
BACnet
DNP3
EtherCAT
EtherNet/IP + CIP
Foundation Fieldbus HSE
IEC 60870-5-101/104
ICCP TASE.2
IEC 61850 (MMS, GOOSE, SV)
IEEE C37.118
(Synchrophasor)
Modbus ASCII
Modbus RTU
Modbus/TCP
OPC-DA
OPC-AE
PROFINET (RPC, RTC, RTA, DCP and PTCP)

Proprietary OT systems/protocols
CSLib (ABB 800xA)
DMS (ABB AC 800 F)
MMS (ABB AC 800 M)
PN800 (ABB Harmony)
SPLUS (ABB Symphony Plus)
ADS/AMS (Beckhoff)
CygNet SCADA (CygNet)
DeltaV (Emerson)
Ovation (Emerson)
SRTP (GE)
Experion (Honeywell)
ADE (Phoenix Contact)
CIP extensions (Rockwell/AB)
CSP (Rockwell/AB)
COMEX (Schneider Electric Foxboro)
OASyS (Schneider Electric)
Modbus/TCP extensions
(Schneider Electric)
Telnet extensions (SEL)
Step7 (Siemens)
S7COMM+/OMS+ (Siemens)
Vnet/IP (Yokogawa)

IT Protocols	
AFP	SMTP
BGP	SNMP
DHCP	SSDP
DNS	SSH
FTP	SSL
HTTP	SunRPC
IMAP	Telnet
Kerberos	TFTP
LDAP	
LDP	
MS-SQL	
NTP	
NetBIOS	
OpenRDA	
POP3	
PVSS	
Radius	
RDP	
RFB/VNC	
RPC/DCOM	
RTSP	
SMB/CIFS	

Honeywell

EtherNet/IP + CIP

A secure EtherNet/IP transport provides the following security attributes:

- Authentication of the endpoints — ensuring that the target and originator are both trusted entities. End point authentication is accomplished using X.509 certificates or pre-shared keys.
- Message integrity and authentication — ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS message authentication code (HMAC).
- Message encryption — optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS handshake.
- Inside ODVA's Ethernet/IP Enhancements

Through its reliance on standard Internet and Ethernet standards, EtherNet/IP is the only industrial Ethernet network that is proven, complete and ready for the Industrial Internet of Things.

Source: https://www.odva.org/Technology-Standards/EtherNet-IP/Overview &
CIP Security for EtherNet/IP Illustrates Increased IT/OT Integration By Bill Lydon, Contributing Editor, Automation.com

Honeywell

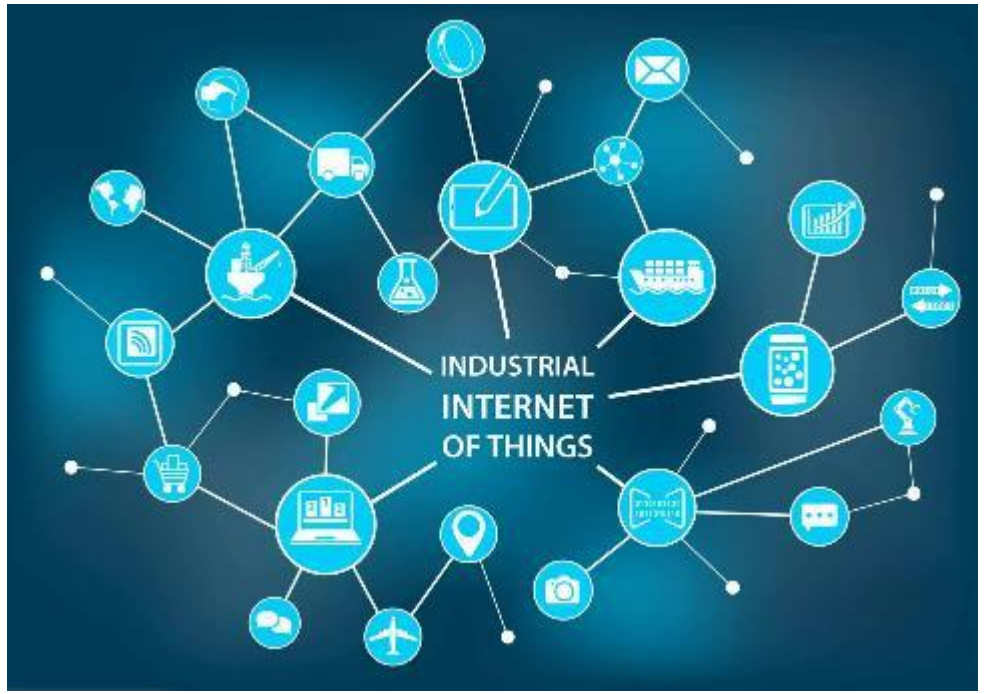
Edge Device Security

The goal of ODVA's cybersecurity enhancements to EtherNet/IP is to extend a defense-in-depth architecture to network communications with and between ICS systems and edge devices.

As attackers become more sophisticated, it becomes more important for a Common Industrial Protocol (CIP) connected device, the final layer of defense, to defend itself; especially in the age of IIoT

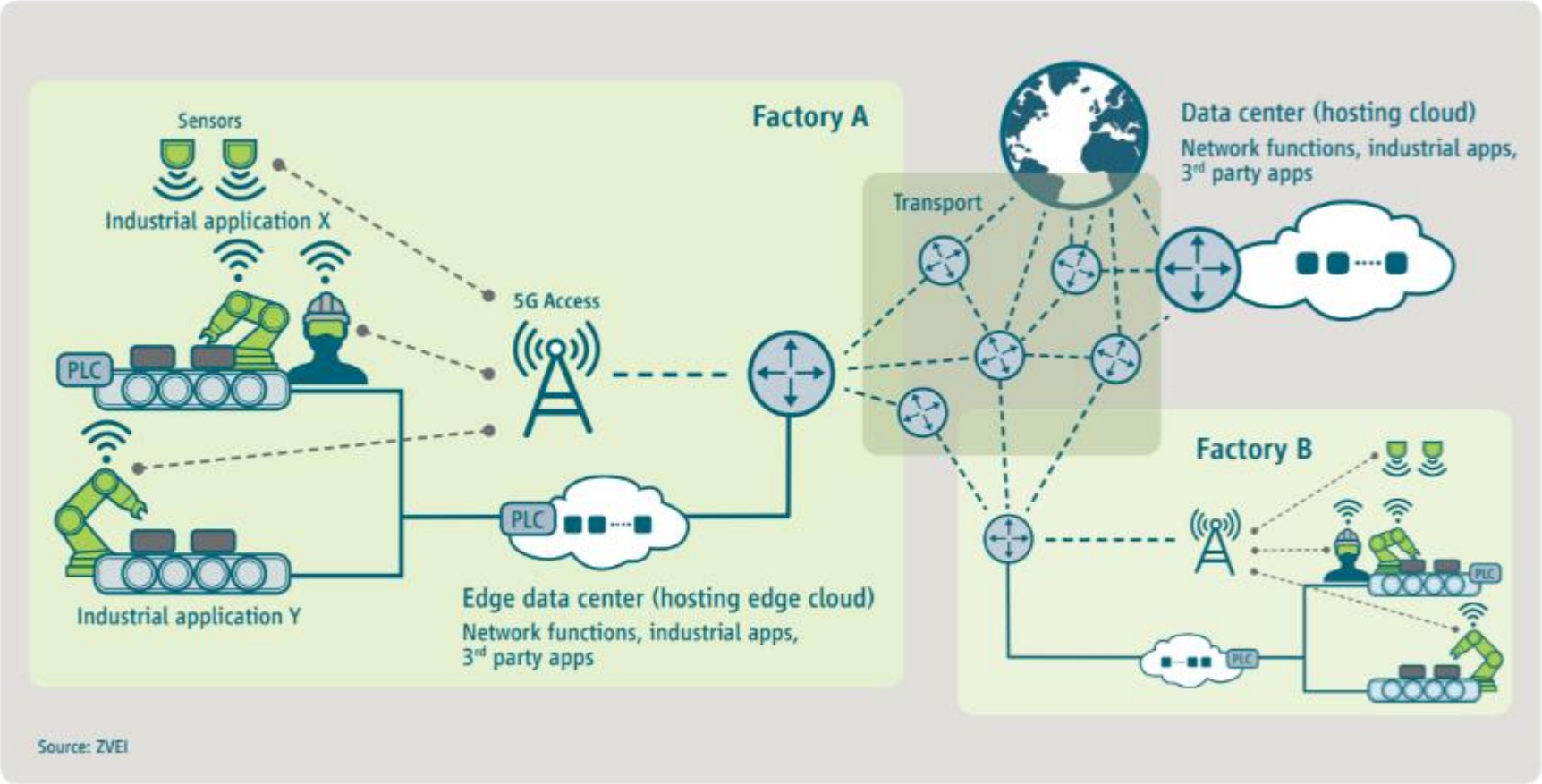
The goal of CIP Security is to enable the CIP-connected device to protect itself from malicious CIP communications. A fully self-defending CIP device would be able to:

- Reject data that has been altered (integrity)
- Reject messages send by untrusted people or untrusted devices (authenticity)
- Reject messages that request actions that are not allowed (authorization)



Source: CIP Security for EtherNet/IP Illustrates Increased IT/OT Integration By Bill Lydon, Contributing Editor, Automation.com

5G for Connected Industries and Automation



Security

5G includes strong E2E security. In particular, mutual authentication between the device and the network is supported. All transmitted data is encrypted E2E between the device and the network. 5G also supports a flexible authentication framework with the Extensible Authentication Protocol (EAP) and strong encryption, while meeting strict latency requirements.

HOWEVER

Honeywell

5G Expands Cyber risk

- The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing.
- 5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances.
- Even if it were possible to lock down the software vulnerabilities within the network, the network is also being managed by software that itself can be vulnerable.
- The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack. Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets.
- Vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT.

Source: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

Honeywell

Hacking Industrial Control Systems

Hacking PLC modbus with mbtget - YouTube
https://www.youtube.com › watch ▾


Dec 15, 2015 - Uploaded by Ozkan Erdogan
Mbtget is a python code that can read and write to/from PLC's. In this example, we will use a **Modbus** PLC ...

Honey, I Hacked The SCADA! : Industrial CONTROLLED ...
https://www.youtube.com › watch ▾


Mar 19, 2016 - Uploaded by RSA Conference
Honey, I **Hacked** The SCADA! : Industrial .... DEFCON 16: ModScan: A SCADA **MODBUS** Network Scanner ...

Modbus PLC Attack Demonstration - YouTube
https://www.youtube.com › watch


May 23, 2017 - Uploaded by Anmol Dudani
This video shows the attack demonstration of **Modbus** PLC using 102 ... DEF CON 26 - Thiago Alves - **Hacking** ...

Hacking PLC and RTU SCADA devices in a lab - YouTube
https://www.youtube.com › watch


Dec 7, 2012 - Uploaded by Jonathan Pollet
Students at our Red Tiger Security SCADA Security Training course are sending custom crafted packets to flood ...

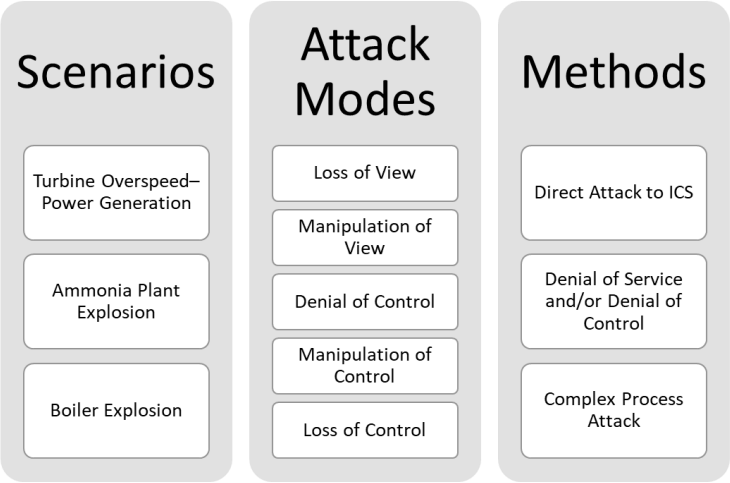
Defocon 16 - Modscan: A Scada Modbus Network Scanner
www.securitytube.net › video ▾

Mar 23, 2012 - Uploaded by SecurityTubeCons
ModScan is a new tool designed to map a SCADA **MODBUS** TCP based network. The tool ... I will also be ...

Attacks on SCADA systems

Supervisory control and data acquisition (SCADA) systems are highly targeted by attackers because controlling vital systems like Nuclear stations or Power plants is very dangerous. The are many attacks that face SCADA systems. These are some of them:

- Denial Of Service
- Databases attacks including SQL injection
- Code execution
- Privilege Escalation
- Buffer overflows



Honeywell

Summary: High-level Challenges on Communications

ICS/SCADA Complexity

- Multiple sites
- Multiple vendors requiring access to assets
- Multiple protocols on ICS network
- Multiple businesses
- Mix of legacy and proprietary equipment

Supply Chain
Mobile Workers

IT/OT Misalignment

- ICS security ownership is not clear
- OT/IT mindsets are very different
- Transition from plant-by-plant to plant-wide security practices

Skilled Resources Shortfall and Budget Limitation

- Cannot place experts at every site
- Manual processes don't scale and only provide limited security
- Multiple security solutions partially utilized

Honeywell

Final Word

Disruption in your connectivity can be as simple as blocking your WiFi