

Industrial Cybersecurity Challenges

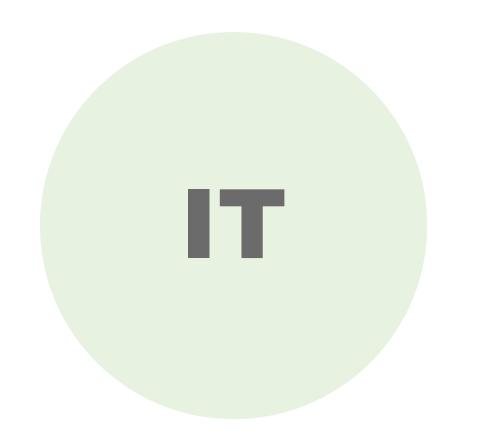
Andreas Reiter RC-AT DI FA DH-GRAZ SAS andreasreiter@siemens.com

Unrestricted © Siemens AG 2019

siemens.com/industrialsecurity

IT – OT?



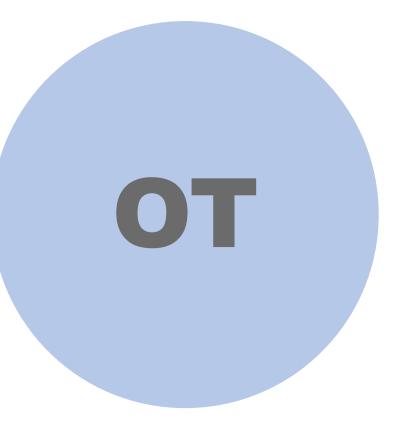


- Dynamic
- Full spectrum of technologies
- Well connected
- Confidentiality, Integrity, Availability
- Data is King

IT – OT?



- Control production floor processes
- Process oriented
- Safety/Availability, Integrity, Confidentiality
- Process is King

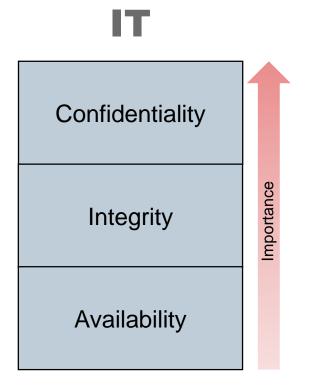


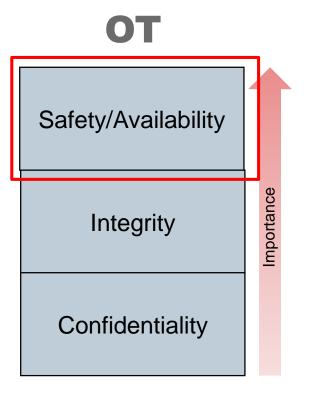
| IT - OT Challenges | | SIEMENS Ingenuity for life |
|------------------------|-------------------------------|--|
| Information Technology | 完 | Operational Technology |
| 3-5 years | Asset lifecycle | 20-40 years |
| Forced migration | Software lifecycle | Usage as long as spare parts available |
| Well integrated IAM | Requirements on Identities | Long living identities (static accounts?) |
| High | Options to add security SW | Low |
| Low | Heterogeneity | High |
| | | |

Unrestricted © Siemens AG 2019Page 42020-02-18

Priorities



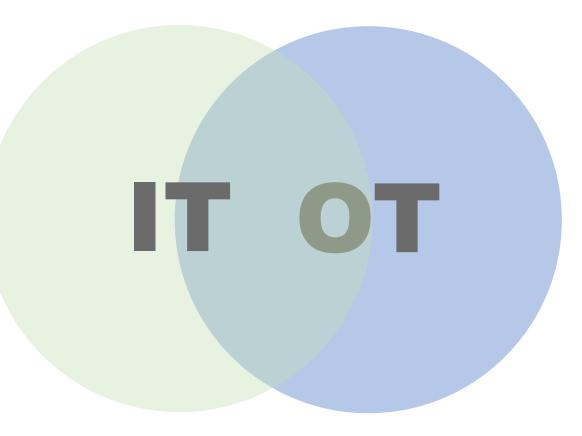




IT – OT?



- Massive data generation
- Big data analytics capabilities
 - Real-time decisions
 - Predictive maintenance
- Increased efficiency and productivity
- Create new revenue streams



Concerns



73% are aware that their attack surface increases

55% have no plans invest, or plan to invest in cybersecurity in the next 12 months

91% are aware that OT security can only be tackled together with IT

Unrestricted © Siemens AG 2019 Page 7 2020-02-18

Andreas Reiter / RC-AT DI FA DH-GRAZ SAS

(Not)Petya (2017)



- Maersk: Petya infected IT infrastructure
- Gates did not open (no data)
- Trucks were locked out

| teps: . Dowmlo help, . Visit | se your key and restore your data, please follow these three easy |
|---------------------------------------|--|
| help, . Visit | |
| | ad the Tor Browser at "https://www.torproject.org/". If you need please google for "access onion page". one of the following pages with the Tor Browser: |
| - | /petya37h5tbhyvki.onion/N19fvE /petya5koahtsf7sv.onion/N19fvE |
| . Enter | your personal decryption code there: |

Ransomware is here to stay



Technology

Ransomware attack takes US maritime base offline

BBC



On Monday January 13, 2020, Picanol Group fell victim to a massive ransomware attack. The attack is causing a serious disruption to activities in Ypres, Romania, and China.

Unrestricted © Siemens AG 2019 Page 9 2020-02-18

Open Industrial Control Systems





Open Industrial Control Systems



| Hamerka | | | | | |
|--|--|---|--|--|--|
| | Locate | Intel | Exploit | | |
| INDUSTRIAL CONTROL SYSTEMS INTERNET OF THINGS HEALTHCARE UPLOAD NMAP SCAN | 40.67619999999994,-73.8736 - 289020 KINGS HENDRIX 2816 ATLANTIC AVE. BROOKLYN N.Y. 50533874405001 | | | | |
| Country = Austria | Map Satellite 7 Secaucus East Orange Kearny | ergen Dergen | Manhasset Roslyn Old Westbury Jericho Stat Lake Success Mineola Westbury Mineola Bethpag | | |
| Device Select an option | vood Irvington D Arabitettike nion Hillside C Arabitettike T Arabitettike Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettike T Arabitettikettikettikettikettikettikettiket | | Elmont State Prof. Wanta | | |
| WAGO Sensatronics Extron Electronics Mikrotik Streetlight | Elizabeth Bayonne NEW JERSEY VIEW VORK ST. GEORGE Linden Google in 2010 100 100 100 100 100 100 100 100 10 | Contraction of the state of the | Woodmere Oceanside Terms of Use Report a map error | | |
| Kesseltronics Unitronics Atvise | Shodan scan for nearby devices | | | | |
| | device:webcam Search | Show Add | | | |

Strong Perimeter Security



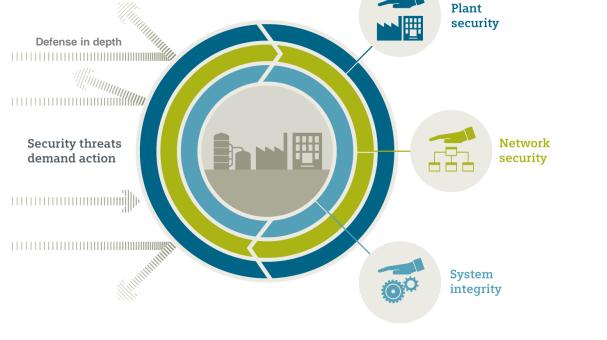


- Analog to air gapping
- Firewalls
- Traffic analyzers
- Strong access management

Defence in Depth



- Know what's going on in your network
 - Network monitoring
 - Log analysis
- "Castle approach"
 - Multiple lines of defense
 - Network segmentation
 - Device security
 - Common cryptographic principles
 - Security-by-design



. . .

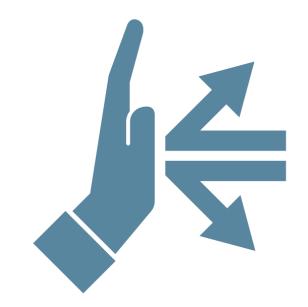


- Be proactive
- Not only scan IT, but also OT networks and components
- Check against known vulnerabilities
 - Open vulnerability databases
 - Vendor specific databases

Processes



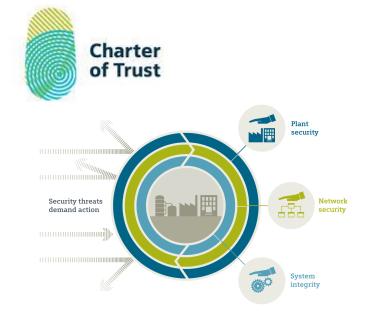
- Security Event Management (SEM)
 - Near real-time security alarms and events
- Security Information Management (SIM)
 - Long-term storage of log data
- Patch management



Siemens DH-Graz



- Founding member of the charter of trust
 - Holistic concepts
 - Think beyond products and services
- Plant Security Services
- Strong Security competence at DH-Graz
 - Security testing
 - International research projects
 - defense in depth
 - controlled access to production networks
 - certification



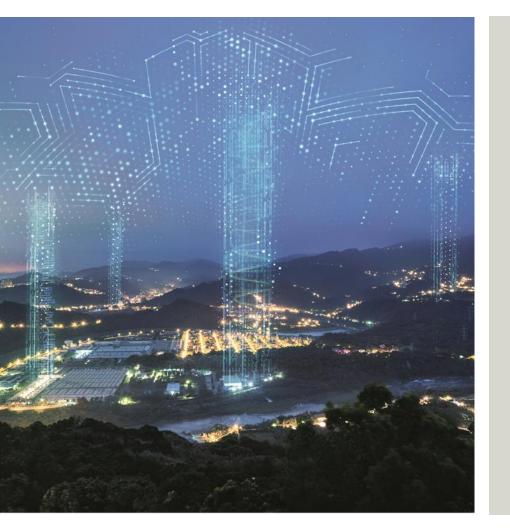
Your Takeaways



- IT and OT environments are converging
 - ...to make better use of data
 - ...to perform data analytics
- More attack vectors
- Be proactive in the definition of your security strategy

Contacts





Andreas Reiter RC-AT DI FA DH-GRAZ SAS

E-mail: andreasreiter@siemens.com

https://www.linkedin.com/in/anreiter/

siemens.com/industrialsecurity