CREDC

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Seminar Series

Cybersecurity for IoT to Nuclear

Fred Cohn, Program Director

Who Am I?

- Program Director, Schneider Electric Product Security Office
  - Cybersecurity Strategy
  - Process (SDL) Deployment and Governance
  - PSIRT - Incident Response, Vulnerability Management, Threat Intelligence
- Previous background:
  - Industrial Control, Programmable Logic Controllers, Industrial Networking
- How did I get involved in security?
  - A funny thing happened . . .

Who is Schneider Electric?

- Schneider Electric in figures:
  - ~€25 billion in sales in FY2016
  - 144,000+ employees in more than 100 countries.
  - ~5% of revenues devoted to R&D
- About our Company:
- Schneider Electric is the **global specialist in energy management and automation**. With revenues of ~€25 billion in FY2016, our 144,000+ employees serve customers in over 100 countries, helping them to manage their energy and process in ways that are safe, reliable, efficient and sustainable. From the **simplest of switches to complex operational systems**, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies reshape industries, transform cities and enrich lives.

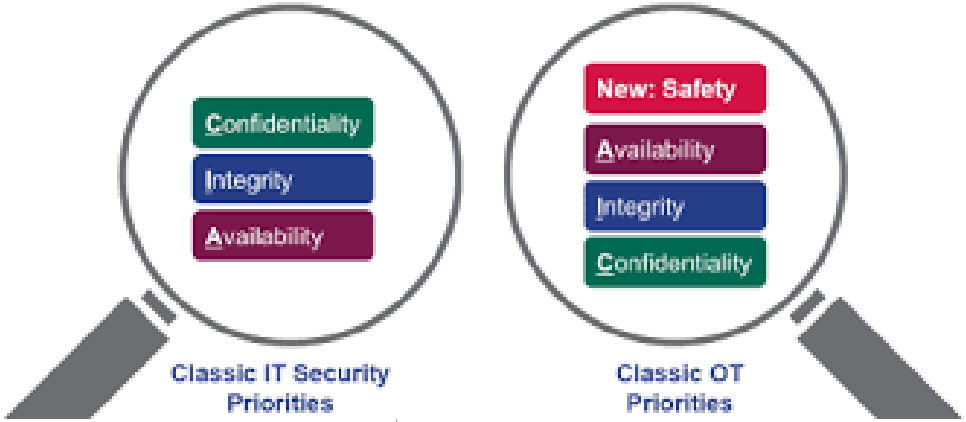
Schneider Electric Offers

- Data Centers:
  - UPS
  - Power Management
  - Cooling
- Building Management:
  - Temperature Control
  - Access Control
  - Metering and Protection

- Electric Utility
  - Protective Relays
  - Substation Controllers
  - Transformers
- Industrial Control
  - Sensors and Actuators
  - Variable Speed Drives and Motor Control
  - PLC's, Motion Controllers, and RTUs
  - DCS
  - Safety PLC and Shutdown Systems

IT vs. OT – Schneider Electric Lives in Both Worlds

- OT = Operations Technology
- Simple answer:
  - IT controls electrons = bits & bytes
  - OT controls molecules = things
- More complicated answer:
  - OT leverages IT technologies; Ethernet, WiFi & Internet stacks, to connect intelligent devices, controllers, and software:
    - Monitor
    - Alarm
    - Control
    - Protect
  - Control vs. Data Centric

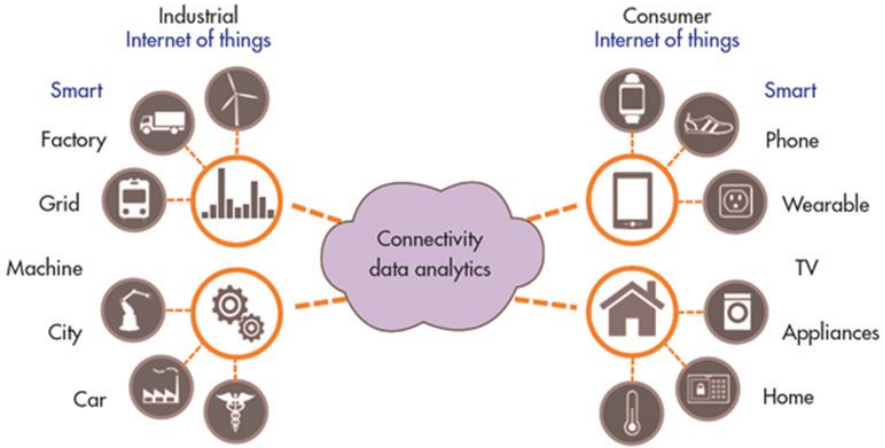


OT is a “Soft” Target for Cyber-based Attackers

- Why OT is a soft target?
  - Older systems; insecure by design
  - Owners don’t have same cybersec skills
  - OT system lifecycle 5-10x longer than IT system lifecycle
  - Shared systems tend to share passwords
  - Naivete! - “We aren’t threatened! Who would attack us? What are they going to do…change the building temperature? Security by Obscurity!”
  - Systems tend to remain unpatched – too risky to patch!
- Good news, if there is any?
  - System attack requires much more process knowledge than typical IT system
  - Systems are designed to fail to a safe condition

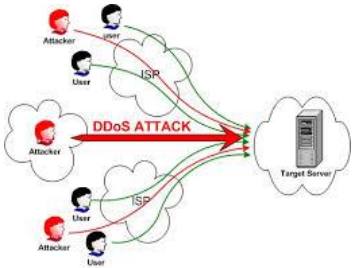
IoT for OT = IIOT

- IIoT – same principles as IoT but different (additional) risks
- Industrial IoT – applying the concept of IoT to Industrial/Commercial Control:
  - Cloud-based Building Management System
  - Facility Monitoring
  - Remote Maintenance
  - Remote Asset Management
  - ADR - Automated Demand Response
  - WAGES tracking
  - Remote robotic surgery – Yikes!



Risks of IIoT

- Personal data can be compromised
- Equipment can be attacked and essential functions can be interrupted
- Data can be manipulated or modified
- Equipment can be damaged!
- Life safety can be impacted!



Schneider’s R&D Approach – It’s a Journey

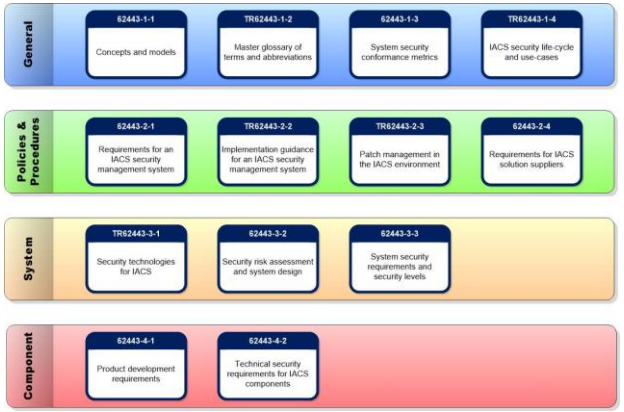
- Standards-based development practices
- Consistency Rules
- Bricks and Platforms
- Innovative Designs Suited for Our Markets
- Research to apply IT Security Practices/Technologies to OT environments

Standards Based Development Approach

- Corporate Policy that all R&D Projects must follow SDL:
  - Initially based on ISO 27034, while a few groups leveraged ISASecure
  - Migrating to IEC 62443-4-1 for all R&D
  - ISO 30111 for Vulnerability Management
- SE IT organization embracing the methodology
- Some R&D departments are SDLA certified

IEC 62443-4-1 Practices

- Security Management
- Security Requirements
- Secure by Design
- Secure Implementation
- Secure Verification and Validation
- Defect Management
- Security Update Management
- Security Guidelines

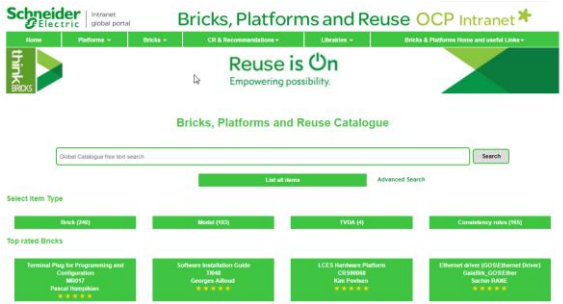


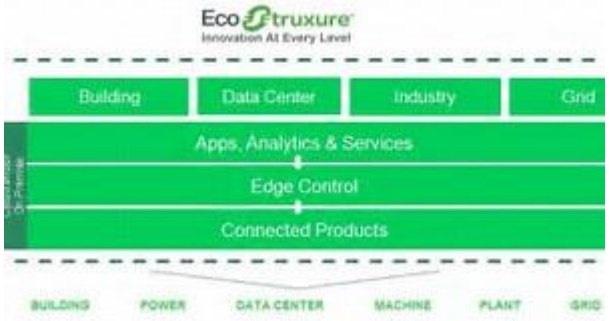
Consistency Rules

- Rules that govern technical choices:
  - Marketing or Technical
  - All segments or segment-based
  - Factored into requirements and checked at early development stage
  - Examples (in development):
    - Robustness testing
    - Software signing
    - Firmware signing
    - Secure Boot

Bricks and Platforms

- Consistency Library
  - Documents
  - Consistency Rules
  - Code References
  - Bricks
- IoT Platform for Hosted Services – EcoStruxure
  - Communication services
  - User AuthN and AuthZ
  - Data storage
  - Application interface services

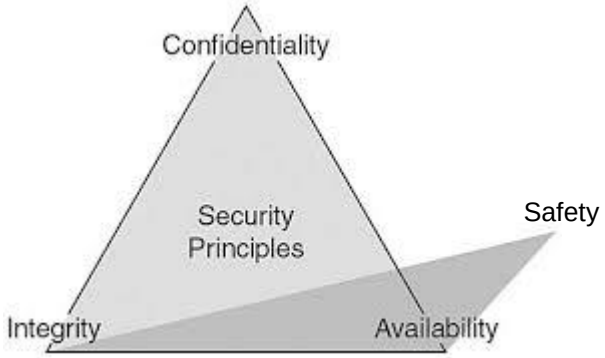




Life Is On Schneider Electric

Innovative Designs – Applying IT Principles to OT Environment

- Software, Device, and Patch Integrity
- User to Machine Authentication and Authorization
- Machine to Machine Authentication and Authorization
- Device Authenticity
- Device Replacement
- Logging and Auditing
- Robustness



Integrity

- We developed a Software Signing Utility to assist development teams.
  - Using Commercial MPKI; Microsoft (or Java) code Signing Techniques
  - Upgrade underway to keep up with Microsoft
- We developed our own Firmware Signing using self-signed MPKI
  - Still immature, but evolving
  - Adoption challenges for our R&D
  - Issues with authentication infrastructure in customer environment
- Patch Signing
  - Depends on Software vs. Firmware

Authentication and Authorization

- All agree on value of certificate-based authentication for U2M and M2M
  - Working on standard approach to allow for interoperability
  - Trying to standardize designs including Secure Elements for future needs
  - Standard crypto library available for all developers
    - Biggest issue is confusion over export/import licensing
- Authorization schemes vary; difficulty with convergence
  - Based on roles
  - Include role in device certificate, or…
  - Centralize system authorization role

Device Replacement

- Consistently, the biggest barrier to applying security technologies and practices
- “How can a failed device be replaced at 3:00AM?”
- Two approaches:
  - System Security Appliance
    - Manages user access, roles, and asset inventory
  - Use certificates in the device
    - Provide a standards-based CA
    - Use standard mechanisms for certificate deployment through CET
      - Working on CET code changes and user documentation

Logging and Auditing

- Created internal standards for logging methods and format for embedded devices.
  - Standard format
  - Protected from modification
- Adoption has just started; limited experience for embedded devices

Secure Industrial Communications

- Protect Confidentiality and Integrity
- Secure Modbus
  - Based on TLS
  - Being submitted to Modbus.org
- Secure EtherNet/IP
  - Being managed by ODVA

Robustness

- Network protocol fuzz testing to prevent DoS
  - Standard TCP and UDP
  - Some industrial protocols
- Standardized on Achilles test; certify devices
  - Alternative, Codenomicon, but no device certification available

Key Areas of Innovation

- Blockchain for Asset Authenticity; what are Use Cases?
- Custom fuzzers for unique industrial protocols
- How U2M and M2M authentication works using certificates when system is not internet connected (or connected intermittently) ((or connected through a gateway))
- How do we validate genuineness of a device that connects to our hosted solutions?
  - Did we manufacture it?
  - Is it our firmware?
- How do we validate integrity of embedded device configuration or application program
- Intersection of Security and Safety

Educate our Customers, Channel Partners, and FSE's

1. Patch Your System
2. Separate the Network
3. Define and Enforce Contractor Guidelines
4. Secure Remote Connections
5. Password Management
6. Educate Your People
7. Monitor Your System

Life Is On | Schneider Electric