Safety First! (because) Injuries Last!

A Cybersecurity Perspective

Fred Cohn, Program Director

Summary

- Critical Infrastructure is becoming a larger target
- Many CI control systems are older and designed without security in mind
- Protecting CI systems “takes a village” – everyone has a role:
  - Ops and Maint dept.
  - Asset owner IT dept
  - OEM and SI

Who Am I?

- Program Director, Product Security Office, Schneider Electric
- Previous background:
  - Industrial Control, PLCs, 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 (2017 figures not official)
  - 140,000+ employees in more than 100 countries.
  - ~5% of revenues devoted to R&D

Schneider Electric Markets and Brands

- Data Center Mgmt
- Building Management
- Electrical Distribution
- Electric Utility
- Industrial Control
  - Process
  - Machine

APC by Schneider Electric

AREVA

SQUARE D by Schneider Electric

Andover Controls
Controlling Tomorrow's World

invensys

Merlin Gerin

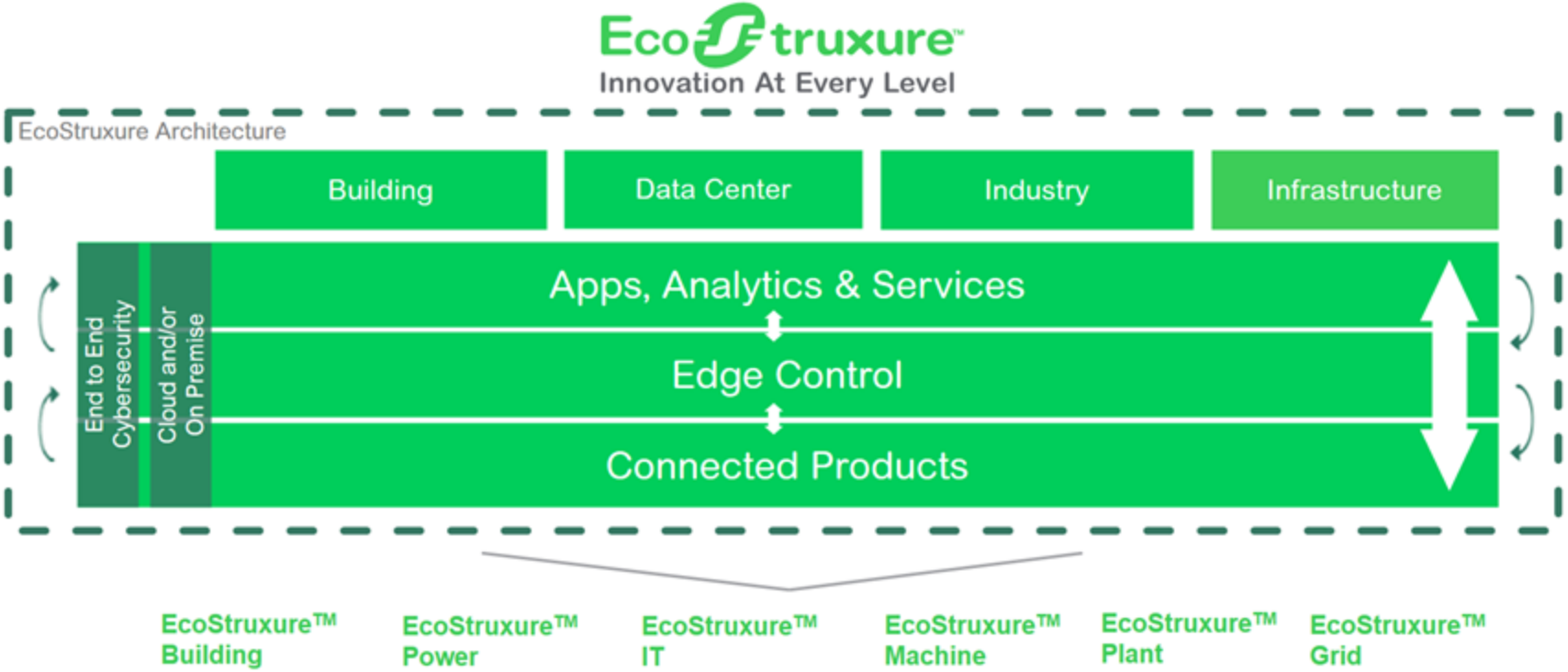
Telemecanique

ASCO

Wonderware by Schneider Electric

Triconex by Schneider Electric

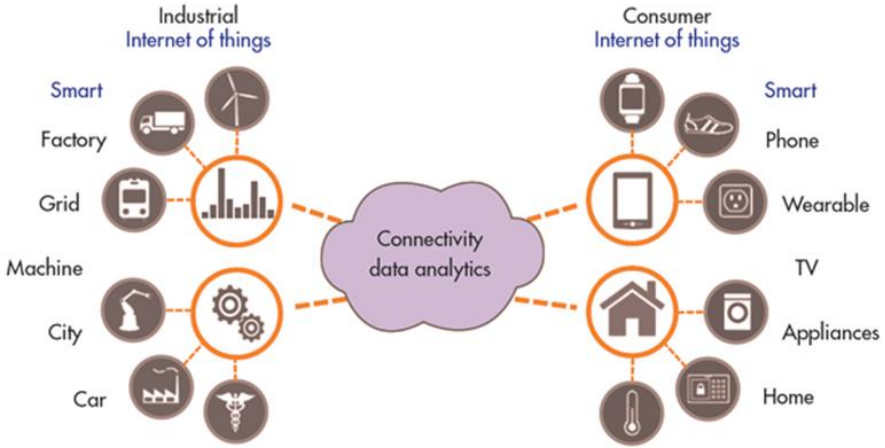
Schneider Electric Strategy – EcoStruxure – Innovation at Every Level



Life Is On Schneider Electric

IoT for OT = IIOT

- Industrial IoT – applying IoT to Industrial Control:
  - Cloud-based Building Management System
  - Facility Monitoring
  - Remote Asset Management
  - ADR - Automated Demand Response
  - WAGES tracking
  - Remote robotic surgery – Yikes!



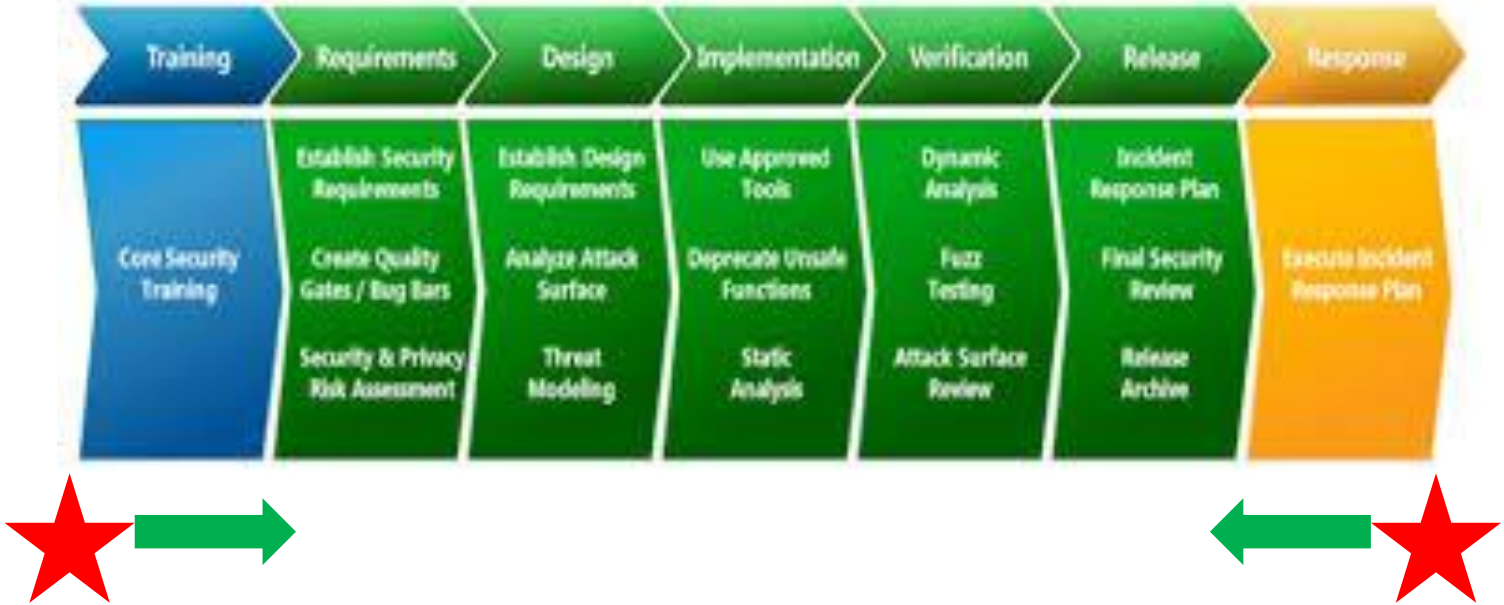
OT is a “Soft” Target for Cyber-based Attackers

- Why OT is a soft target?
  - Older systems; insecure by design
  - OT system lifecycle 5-10x longer than IT
  - Shared systems -> shared passwords
  - Systems aren’t patched – too risky!
- Good news, if there is any?
  - System attack requires process knowledge
  - Systems are designed to “fail-safe”

Schneider Electric's Approach – It's a Journey

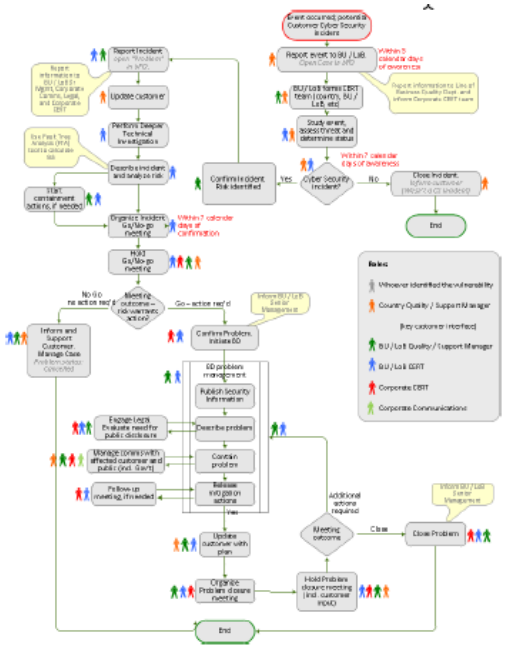
- Standards-based practices
- Rules, Bricks & Platforms
- Alignment Between IT and R&D
- Customer Education and Support

How Our Journey Began – Outside In



First Issue – Vulnerability Management

- Large legacy Installed base
- Addressed Vulnerability Reports
- Created a process:
  - Started with Corporate Quality – I2P
  - Adapted from our Safety Alert process
  - Corporate Web Presence



Educate Our Customers – Protect Their Systems

- Air-gap is a myth!
- Isolate your systems using DMZ's and Firewalls
- Assess Your Inventory – big issue!
- Patch!
- Monitor

Adoption of SDL Practices

- Corporate Policy – based on ISO 27034
- Incorporated into our R&D Frameworks:
  - Waterfall
  - Agile
  - Brand Label
- Built-up staff
  - Central - Experts and Analysts
  - Distributed - Security Advisors and Architects

Standards Based Development Evolution

- Policy – Standards Conformance:
  - ISO 27034 -> 62443-4-1
  - 62443-2-4 for Projects
  - ISO 30111 for Vulnerability Management
- Certification where appropriate

Process <-> Functionality

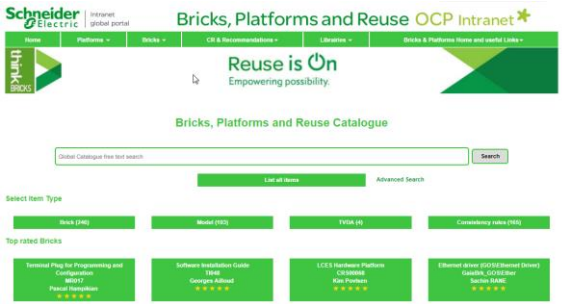
- Incorporate Cybersecurity Standards – 62443, 62351
- Biggest challenge – simple home device -> nuclear control/safety system
- Leveraged Our Existing Invariant and Brick methodology
  - Consistency Rules
  - Bricks and Platforms

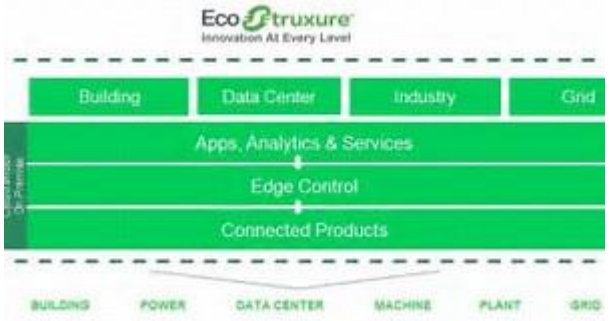
Consistency Rules

- Rules that govern technical choices:
  - Marketing
  - Technical
- Factored into requirements
- Examples (in deployment):
  - Robustness testing
  - Software & Firmware signing
  - Secure Boot

Bricks and Platforms

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

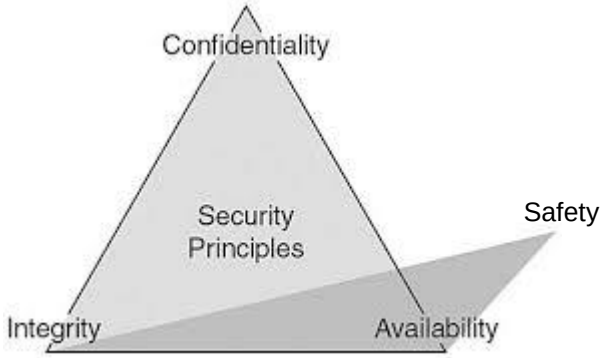




Life Is On Schneider Electric

Innovative Designs – Applying IT Principles to OT Environment

- Software, Device, and Patch Integrity
- User to Machine AuthN and AuthZ
- Machine to Machine AuthN and AuthZ
- Device Authenticity
- Faulty Device Replacement
- Logging and Auditing
- Robustness



Alignment Between IT and R&D

- R&D Source Code Repositories
- Manufacturing and Logistics
- Field Service and Project Delivery
- Customer Requirements

Tricon

- Very skilled “bad” actor
- Apparently, in the system a long time
- Able to load malware on Tricon SIS
  - Keyswitch in unprotected mode
  - Network not optimally isolated
- System performed plant shut down “as designed”

Educate our Customers, Channel Partners, and FSR’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

Lessons Learned

- Bad guys are out there – and they're skilled!
- Control systems are vulnerable:
  - Old
  - Poor security design
- OEM's have a role, but it takes a new mindset:
  - Upgrade/patch where possible
  - Isolate where not possible
  - Educate everyone
  - Monitor everywhere

Life Is On | Schneider Electric