Vincent Turmel (Siemens) – Erik Anderson (Intel Security)

Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Agenda

• Why is IoT present in an industrial environment?

• Why is IoT a Security Threat?

• How can we protect our plants

• Challenges and solutions in adopting standard IT controls

• Conclusion
Internet of Things
Defining the way forward in industry in the internet age

Devices are increasingly connected in the home: smart TV, fridge, thermostat, door locks, light bulbs (!)

It is coming to the plant environment because it brings tangible benefits. It allows:

1. Horizontal integration of the value-add networks
2. Vertical integration and networked production systems
3. End-to-end engineering across the entire value chain

The modern age requires real time KPI updates
The next industrial revolution

From Industry 1.0 to Industry 4.0

**First Industrial Revolution**

Based on the introduction of mechanical production equipment driven by water and steam power.

*First mechanical loom, 1784*

**Second Industrial Revolution**

Based on mass production achieved by division of labor concept and the use of electrical energy.

*First conveyor belt, Cincinnati slaughterhouse, 1870*

**Third Industrial Revolution**

Based on the use of electronics and IT to further automate production.

*First programmable logic controller (PLC) Modicon 084, 1969*

**Fourth Industrial Revolution**

Based on the use of cyber-physical systems.

*Degree of complexity*

*Source: DFKI (2011)*
Example of the Future Manufacturing

I am a car body and I will tell you what’s next.

I am the conveyor and I will go to energy saving mode.

I am robot 1 and need repair.

we are robot 2 + 3 and we need special parts.

I now see in real time what’s going on.

The main challenges and drivers in the industrial environment

Reducing the time to market
- Shorter innovation cycles
- More complex products
- Larger data volumes

Enhancing flexibility
- Individualized mass production
- Volatile markets
- High productivity

Increasing efficiency
- Energy and resource efficiency as key competitive factors

Safety & Security
Objectives of Safety & Security in industrial automation

**SAFETY**

Prevent danger/hazards to people and the environment

Objectives
- Robustness
- Reliability

**SECURITY**

Protect systems against misuse and unauthorized access

Objectives
1. Availability
2. Integrity
3. Confidentiality
Until recently, cybersecurity has focused on a limited number of end points. This is no longer adequate as the physical and virtual worlds combine at a large scale. Need for new security frameworks that span the entire cyber physical stack, from device-level authentication and application security, to system-wide assurance, resiliency and incidence response models.

Cyber security is an enabler for IoT. Achieving the IoT vision is not possible without putting adequate security measures in place.
What does an Industrial Environment look like today?

Figure 1. High-level design based on the Purdue model.
Difference between Industrial and IT Environments

What do we find in industrial environments?

- Much more machines than humans
- Different devices & protocols
- Mix of operating systems & vendors
- No direct access (firewalls, gateways)
- IPv4 wired-/ wireless- & serial-networks
- Harsh environment
- Real time and safety
- 24/7 operations with focus on availability
Today’s best practices to adopt standard IT controls

Security Monitoring with SIEM
- Rugged hardware to collect data from distributed industrial devices
- Create configurations and rules for industrial automation
- Ensure availability i.e. not invasive to real time communication

Perimeter protection
- Understand industrial protocols (S7, Profinet, Ethernet-IP, Modbus, OPC)
- Create signatures for industrial targeted attacks and update configurations
- Ensure availability i.e. don’t block if you are not 100% sure

Patching
- 24/7 operation allows patching only during maintenance time
- Patches must be tested and vendor approved
In the future, how to secure the industrial automation

- Integrated safety and security strategies, architectures and standards
- Unique IDs & “security passport” for products, processes and machines
- Retrofit/migration strategy to improve the security of current facilities
- User-friendly safety and security solutions
- Know and quantify the business impact (direct and indirect cost)
- Protection against product piracy
- Training for employees
- Data protection

Source: Action in the field of safety and security (Industrie 4.0 Working Group)
Security Opportunities in ICS
Security Measures May Be More Effective in Industrial Environments

Strict Isolation
- Well-defined communication at boundaries

Regulated Change
- Infrequent changes

Focused Functionality
- Fixed set of applications

Restricted User Activity
- Well-defined user roles

Firewalls
- Whitelisted communication

Change Control
- Auditing system changes

Application Control
- Whitelisting

SIEM
- User activity auditing
Use Case
Typical Controls

Communication
• Security level network boundaries
• Monitoring data flows

Malware Prevention
• Antivirus
• White-listing
• Removable media
• Blocking
• Scanning

Configuration Control
• Auditing
• File integrity

Audit Logs
• Required
• User Access
• Malware
• System status
• High-Value
• Removable media
• Application events – failures
• Escalated privileges
• Correlated events
• Deviation from baseline
• Storage
• Long-term
• Non-repudiation
We are partners (announced at the Hannover fair 2014)

We use McAfee technology e.g. SIEM for our Security Services

We will jointly develop security solutions
Managed services from the secured SIEMENS Cyber Security Operations Center

Security & industrial automation experts

Secured Connection

Subscribed Customer

AV, WL- Management
Security Monitoring
Firewall Management
Patch + Incident Response
Reporting
McAfee Solution Components
Essential Products

Endpoint Security
- ePolicy Orchestrator
- Endpoint Security
- Integrity Control
- Device Control

SECURITY INFORMATION AND EVENT MANAGEMENT
- Enterprise Security Manager

NETWORK SECURITY
- Network Security Platform
- Application Data Monitor

Two-way integration between McAfee components and SIA partners
Air-gap implementation for isolated systems
Support for industrial products and protocols
Flexible and expandable solutions
Virtual appliances

Source: MSI Survey
McAfee SIEM
Industrial-Specific Points

Event Management
- Aggregation
- Normalization
- Correlation

Log Management
- Long-Term Storage
- Non-Repudiation

Actions
- Alarms
- Automated Response
- Watchlists

Security Information and Event Manager
ePolicy Orchestrator
Centralized Endpoint Security Management

Antivirus - Endpoint Security Threat Prevention
Application Whitelisting – Integrity Control
Device Control – Device Control
File Integrity Monitoring – Integrity Control

A single point managing endpoint security
Reduced workload
Faster deployment
Tighter integration
Network Security
Perimeter and Internal

Network Security Platform
Perimeter Network Intrusion Prevention
North-South Protection and Detection

Application Data Monitor
East-West Detection
Security Information and Event Management

Architecture - Details

SIEM

Events
- System events
- Network devices
- User activity
- Security events – endpoint, firewall, correlation
- Configuration changes

Log management
- Long-term storage
- Non-repudiation

Event forwarding
- IT personnel can monitor without access to ICS
- Alerts/alarms to incident response
Flow/Application Data Monitor

Passive Monitoring
- Flow analysis
- Deep packet inspection – application level
- Built-in ICS rules/protocols

Collection
- Port mirroring (SPAN)
- Network taps
- Plant network, Ethernet control networks

Integration
- Flow
  - Built-in to SIEM receiver
- ADM
  - Optional appliance for SIEM
  - Managed from SIEM interface
  - Full integration with SIEM Advanced Correlation Engine and watchlists
Endpoint Protection
Architecture - Details

Endpoint Security

- Endpoint security
- Application Control
- Device control
- File integrity monitoring (HIDS)
- Antivirus

Scope

- Full implementation in plant network – servers and workstations
- Control system- servers, workstations, HMI – simple deployments
- Embedded devices – where feasible
- Application control – compatible with many legacy systems

Integration

- Managed (ePO) or standalone
- Event logs to plant SIEM
- ePO tagging from SIEM
Modular Security Service Portfolio with Intel/McAfee Technology (Aligned with NIST and IEC62443)

Identify

- Assessments (ISO2700, IEC62443, PCS7)

Protect & Detect

- Training for operators
- Review & implement ICS policies & secure network concepts
- Patching and backup
- Hardening of devices and systems
- Install & manage Intel Security technology

Respond & Recover

- Incidence response and data recovery
Conclusions

We can ..
apply standard IT products & methodologies for INDUSTRIE 4.0

We need ..
Know-how on automation systems and security

We ..
are strong partners to secure our factories today and in the future

Let’s build this future together!
Contact

**Vincent Turmel**
Cyber-Security Consultant
Siemens Industry, Inc. / DF CS DS PSS
1201 Sumneytown Pike
Spring House, PA  19477
Phone: +1 610 470 3650
E-mail: vincent.turmel@siemens.com

**Erik Anderson**
Sales Engineer, OEM Embedded Sales
Intel Security
Mobile: +1 724 814 6870
Email: Erik.Andersonl@intel.com