IT Security in “Industrie 4.0”

Prof. Dr. Michael Waidner
TU Darmstadt & Fraunhofer Institute for Secure Information Technology
1. What is Industrial IT Security?

2. Research Agenda for Security in Industrie 4.0

3. We need European Coordination, Standards, Players
Industrie 4.0: The 4th Industrial (R)evolution

Security in Industrie 4.0 = Security in Cloud, Big Data, CPS, ICS, ...

Survey Across German Industry and Academia (2013)

Security is Perceived as Major Barrier for Industrie 4.0

- Doubts over IT security
- Lack of standards
- Demand for highly qualified people
- Insufficient ICT infrastructure
- High investment costs

Source (in German): VDE-Trendreport 2013, Befragung Unternehmen und Hochschulen
Priorities of Industrial IT Security

1. Loss of Integrity
   - Sabotage
   - Unnoticed reduction in quality of product
   - Unnoticed increase in resource consumption
   - Use of counterfeit components / services

2. Loss of Availability
   - Shutdown in an unsafe state
   - Loss of productivity

3. Loss of Accountability
   - Inability to produce legally required evidence
   - Inability to determine and attribute problems

4. Loss of Confidentiality
   - Industrial espionage
   - Product piracy
   - Violation of employee / client privacy
Examples

U.S. warns SCADA systems at risk
Federal cybersecurity group issues warnings about tools that could be used to attack critical infrastructure systems like power companies and utilities, following release of exploits.

To Kill a Centrifuge
A Technical Analysis of What Stuxnet’s Creators Tried to Achieve
Ralph Langner
November 2013

The SCADA That Didn’t Cry Wolf
Who’s Really Attacking Your ICS Equipment? (Part 2)
Kyle Wilhoit

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits
First hacktivist-style assault to use malware?
By John Leyden, 29 Aug 2012

© Fraunhofer-Gesellschaft 2014
Recommendations, Standards, Surveys

VDMA: Survey

Fraunhofer SIT:

BSI: ICS Security Kompendium

Sicherheit und Industrie 4.0

VDI 2128

NIST SPUB 800-82 Draft

NIST SPUB 800-160 Draft

IEC 62443

Fraunhofer SIT
Evolution of Industrial IT Security
Follows (slowly) the overall development of IT security

State of the Art IT, ca. 1964

State of the Art IT, ca. 2014

Security for Industrial IT Today

Security for “Industrie 4.0”

- Hacking cyber-physical systems
- No air gap, everything connected
- Core services are outsourced
- Shared ownership of machines
- Loss of perimeter control

- Functions and data move to cloud
- Need for trusted identities and trustworthy infrastructure
- Security by Design to cope with complexity
- Big Data causes confidentiality problems
1. What is Industrial IT Security?

2. Research Agenda for Security in Industrie 4.0

3. We need European Coordination, Standards, Players
Topics for a Research Agenda

Security by Design for Systems & Integration

Strategies for Transition and Introduction of Industrie 4.0 Security

Trustworthy ICT Infrastructures and Secure Identities

IP Protection, Anti Piracy & Accountability / Provenance

Usability and Security & Privacy

Define Liability, Privacy, Data Protection in Industrie 4.0

Source (in German): Sicherheit und Industrie 4.0, Fraunhofer SIT, Darmstadt 2014
1. What is Industrial IT Security?
2. Research Agenda for Security in Industrie 4.0
3. We need European Coordination, Standards, Players
Consortia in Germany, EU and USA
Unclear level of coordination and cooperation

2013: BITKOM, VDMA, ZVEI + ABB, Bosch, Festo, HP, IBM, Infineon, Phoenix Contact, SAP, Siemens, Telekom, ThyssenKrupp, Trumpf, Volkswagen, Wittenstein + ...

2009: Research cluster

Opportunities for Coordination and Cooperation

- Standards, processes and tools for Security by Design, test criteria and labs, ...
  - Beyond IEC/ISA 62443

- Cross-organizational trust is key for federation and integration
  - Trusted identities and identity management
  - Trusted platforms and remote attestation capabilities
  - Trusted core networks and trusted integration
  - Cross-organizational “smart” security monitoring
  - Cross-border trust, security, security monitoring

- EU-level vendors need EU-level security standards
  - Including security and crypto standards for government use
  - Increase European participation in intl. security / crypto standards
  - Create incentives for improving security and privacy