Security for Industry 4.0
Trends -- Challenges -- Opportunities

Dr. Wolfgang Klasen, Siemens Corporate Technology and Member of the German Platform Industry 4.0
Increasing intelligence and open communication drive security requirements in various industrial environments.
Our industrial society confesses a growing demand for IT-Security

**IT Security trends are determined by drivers such as**

- Industry infrastructures changes (Digitalization)
- More networked embedded systems
- Increasing device-to-device communication
- Need to manage intellectual property

**And**

- Increasing international organized crime
- Privacy
- Compliance enforcement
- Cyber war fare
- Cloud/Virtualization
- PDAs, Smart Mobiles
- Social Networks / data mining concepts
- ...
Productivity, speed and flexibility remain the biggest challenges for production industries …

Increased competitiveness

- **Quality**: Closed-loop control and comprehensive traceability become quality characteristics
- **Productivity**: Energy efficiency and resource efficiency are critical competitive factors
- **Speed**: Shorter innovation cycles for ever more complex products
- **Flexibility**: Individualized mass production in increasingly volatile markets

… but the focal points of these requirements are changing in the wake of digitalization
Digitalization meets industry: The German concept of “Industrie 4.0” – Seamlessly connecting and improving all steps along the plant lifecycle

“Industrie 4.0”
Merging the real plant with its digital twin – consistent data on all levels and throughout all life cycle phases by integrating engineering software and plant automation

Low CAPEX, optimal OPEX
The Internet is revolutionizing the business world and creates major challenges and opportunities for manufacturing companies:

- Customers are increasingly able to tell their manufacturers directly via the net, what exactly they want and when.
- Formerly isolated processes are getting connected through internet-based services influencing B2C and B2B.
Cyber Physical Systems include physical and digital representation.

Cyber-Physisches System (CPS) contains all information on:
- software / HW
- mechanical devices
- electronics
- automation, HMI
- safety, security
- maintenance
- geographical information
- identities
- status information
- release information
- interfaces
- …

The digital twin will be updated and maintained across the entire life cycle:
- design
- production planning
- production engineering
- production
- services
Security within Industry 4.0:
Security by design & security by default

Security by design as a superior principle
- Subsequent enrichment of systems is not sufficient.
- Security measures have to be integrated (up to application level).

Adaptive security architectures
- Agile security profiles have to be adaptable in a dynamic way.
- Fast configuration must include security.

Security for the digital model
- Security for the physical instance, its digital twin and their interactions must take place in a concerted way.

Prevention and reaction are still needed
- Security will remain moving target. There will be no final I4.0 security solution without a need for further measures.
The Future of Industry: 
Security for Industry 4.0 – (some) constraints and requirements

**Authentication and Secure Identities for Devices**
Unforgeable identities and trust anchors are needed. Keys respectively security credentials must be bound to the device.

**B2B vs. B2C communication**
Individual and short-term consideration of customer requests (“batch-size 1”) need enhanced security.

**IT Security as enabler of business models**
Digitalization of business processes often mandate additional measures regarding IT security. Ease of use and plug & operate are important pre-requisites for the acceptance of security measures.

**Standardization enables secure infrastructures**
Security requires standardized specifications of interfaces and protocols to support requirements and to negotiate and operate security profiles (security semantics) between different domains.
Different factors are driving the research demand for IT Security

<table>
<thead>
<tr>
<th>New Functionality</th>
<th>Security Use Case</th>
<th>Quality of Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Device connectivity, IP to the field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Connectivity of devices and systems to public networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Data analytics, predictive maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 5G</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Know-how protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Industry 4.0 scenarios, IoT,…</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Discovering new/additional threats</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **60 Billion Intelligent Devices**
- **Microcontrollers & microprocessors**
- **Controllers & smart sensors**
- **Static devices**
- **Mobile devices**
- **Static info**
- **Mobile info**

- **Examples**
  - Robust
  - Easy to use
  - Long term security
German National Funded Project: IUNO

Trust in Industry 4.0 requires adequate security measures

Basis of the project are four I4.0 application scenarios:

- Customer individual production
- Technology market place
- Remote access and trusted partners
- Visual security control center for production

IUNO follows the **security-by-design principle** to consider appropriate security measures for the application scenarios from the beginning (threat and risk assessment) until the end (evaluation of integrated security measures).

Project result will be transferred to small and medium enterprises.
Setting standards requires engagement of all stakeholders.

Security standards need global acceptance

- Increasing need to protect intellectual property and business cases with globally defined and accepted quality
- Specific standards and guidelines regarding security and privacy are getting established

Regulatory:
FDA, NERC CIP, CFATS, CPNI, KRITIS

Standards relevant for secure automation:
ISA 99, IEC 62443, HIS, SAE J3061, …

<table>
<thead>
<tr>
<th>Examples of organizations issuing security standards or guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global</strong></td>
</tr>
<tr>
<td>IEC</td>
</tr>
<tr>
<td>ISO</td>
</tr>
<tr>
<td>JTC1</td>
</tr>
<tr>
<td>IETF</td>
</tr>
<tr>
<td>NERC</td>
</tr>
<tr>
<td>ISA</td>
</tr>
<tr>
<td>HIPAA</td>
</tr>
<tr>
<td>DIACAP</td>
</tr>
<tr>
<td>HIPAA Health Information Privacy &amp; Accountability Act</td>
</tr>
<tr>
<td>SAE</td>
</tr>
</tbody>
</table>

Unrestricted © Siemens AG 2016

Page 12 | June 2016

Dr. Wolfgang Klasen
Industrial Security
Enhanced Defense in Depth will be Based on IEC 62443

- Intelligent physical access to buildings and plants
- Self synchronizing access control
- Self learning security management processes
- Dynamic threat analysis and adaption
- Dynamic, flexible network architectures
- Permanent monitoring of networks and communications
- Protection and proof of the integrity of the overall system during the hole lifecycle
- Unambiguous and secure integrity of products, processes and machines