Industry 4.0 from an IoT security standpoint

Dr. Evangelos Gazis
Chief Architect IoT Security
ENISA IoTSec Expert Group
Key questions for today’s session

Industrie 4.0 connects humans, machines, processes, and the flow of goods along value chains

- Which security requirements do we expect for this infrastructure and how can such an infrastructure be established?
- How can we assure a high trust level along the value creation network

Security by design has to be the superior principle

- How can security-by-design be accomplished for the complete life cycle?
- How does a road map for an Industrie 4.0 security ecosystem look like?

Is security really an issue for the value chain?

~ 80% of data breaches have a supply chain origin

~ 45% of data breaches leveraged components of a (current or past) partner

~ 70% of companies lack visibility in their supply chain

~ 60% of companies lack an appraisal process for the cybersecurity of its partners

~ 40% of companies surveyed suffered a data breach in the last 12 months

~ 40% of companies surveyed had financial losses 1-10 MUSD

[1] SANS Institute, “Combatting Cyber Risks in the Supply Chain”
Challenges and drivers to security in Industrial IoT

Challenges
- Lack of visibility
- Lack of transparency
- Lack of alignment
- Lack of controls

Drivers
- Internet of Things (instrumentation and interconnection)
- Digitization (code as the innovation engine)
- 3-D Printing (fine-grain embedment)
Huawei’s supply chain situation

**Huawei Global Supply Network**

- **Source:**
  - US: 32%, the largest material source
  - Taiwan, Japan & Korea: 28% materials
  - Europe: 10%
  - Mainland China: 30%

<table>
<thead>
<tr>
<th>Supply Center</th>
<th>Reverse Center</th>
<th>Local EMS</th>
</tr>
</thead>
</table>
| - China (Delivery for the globe)  
  - Europe (Delivery for West Europe & North Africa)  
  - Latin America (Delivery for America, except Brazil)  
  - Brazil (Delivery for Brazil)  
  - India (Delivery for India)  
  - Dubai (Delivery for Middle East) | - China  
  - Mexico  
  - Europe | - Brazil, Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery |

Supply Center:
- China (Delivery for the globe)
- Europe (Delivery for West Europe & North Africa)
- Latin America (Delivery for America, except Brazil)
- Brazil (Delivery for Brazil)
- India (Delivery for India)
- Dubai (Delivery for Middle East)

Reverse Center:
- China
- Mexico
- Europe

Local EMS:
- Brazil, Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery
Huawei’s approach to supply chain security

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Weight</th>
<th>Percentage</th>
<th>Weighted Score</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security agreement</td>
<td>7%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Security system</td>
<td>12%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Product development</td>
<td>18%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Security test</td>
<td>20%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Third party software security</td>
<td>6%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Delivery security</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Product service security</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Vulnerability advisory and emergency response</td>
<td>16%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Traceability</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Personnel management</td>
<td>6%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This audit checklist includes 10 items and 49 questions, each of which weights 5% to 15% of the total score. There are 1 to 10 questions in each item to evaluate the supplier’s cyber security.

<table>
<thead>
<tr>
<th>Weighted Score</th>
<th>Grade</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 70%</td>
<td>D Failed</td>
<td>High risk</td>
</tr>
<tr>
<td>≥ 70%</td>
<td>C Normal</td>
<td>Medium risk</td>
</tr>
<tr>
<td>≥ 80%</td>
<td>B Good</td>
<td>Low risk</td>
</tr>
<tr>
<td>≥ 90%</td>
<td>A Excellent</td>
<td>Benchmark</td>
</tr>
</tbody>
</table>
Key supply chain aspects of security

Risk management aspects
- Secure environment
- Secure development

Authenticity
- Component (i.e. asset)
- Supplier (i.e. stakeholder)
- Interaction (i.e. trust in the supply chain)

Industrie 4.0 vision

Dynamic online/semi-online system

- **Trust**
  - Suppliers
  - Partners
- **Trustworthiness**
- **Identification**
  - Across organizations
- **Interactions**
  - Business purpose & relevance
Industrie 4.0 reference model
Industrial Internet Consortium threat model
Principles of security design for industrial IoT

Online trust management
- Identity management system
- Certificate management system
- Key management system

Online policy enforcement
- Policy provision (e.g. authentication, access control, etc.)
- Policy enforcement

Online intelligence management
- Knowledge management on threat and vulnerabilities

Online adaptation
- Statistical analysis at multiple levels
- Online model learning
## Pillars of security architecture for industrial IoT

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security-by-design</strong></td>
<td>• Security aspects MUST be integrated in requirements management</td>
</tr>
<tr>
<td><strong>Secure defaults</strong></td>
<td>• Consideration of secure defaults in system/process design</td>
</tr>
<tr>
<td><strong>Reliable asset identification</strong></td>
<td>• Tamper-proof identification framework</td>
</tr>
<tr>
<td></td>
<td>• Interoperable identity schemes</td>
</tr>
<tr>
<td><strong>Compartmentalization of infrastructure</strong></td>
<td>• Segregation and isolation</td>
</tr>
<tr>
<td><strong>Policy enforcement</strong></td>
<td>• Monitoring and analysis of asset interactions (e.g., DPI)</td>
</tr>
<tr>
<td></td>
<td>• Enforcement of policy (e.g., hardening, configuration templates, etc.)</td>
</tr>
<tr>
<td><strong>Testing and validation</strong></td>
<td>• Internal assessments (e.g., penetration tests, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Independent assessments (e.g., reviews, audits, etc.)</td>
</tr>
</tbody>
</table>
Secure development throughout lifecycle processes

<table>
<thead>
<tr>
<th>Primary Lifecycle</th>
<th>Supporting Lifecycle</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Acquisition</td>
<td>• Audit</td>
<td>• Management</td>
</tr>
<tr>
<td>• Supply</td>
<td>• Configuration Management</td>
<td>• Infrastructure</td>
</tr>
<tr>
<td>• Development</td>
<td>• Joint Review</td>
<td>• Improvement</td>
</tr>
<tr>
<td>• Operation</td>
<td>• Documentation</td>
<td>• Training</td>
</tr>
<tr>
<td>• Maintenance</td>
<td>• Quality Assurance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Problem Solving</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Validation</td>
<td></td>
</tr>
</tbody>
</table>

Industrial value chain design vis-à-vis security design

Cybersecurity Governance

Cybersecurity Framework
- Identify
- Protect
- Detect
- Respond
- Recover

Assets and Processes
- Product Design
- Process Design Plant Design
- Engineering Commissioning
- Operation
- Service

Suppliers
Partners
Service Providers
Authorities
From static chains to self-balancing networks of value
From static chains to self-balancing networks of value

Manufacturing
- Labor
- Materials
- Supplies
- Processes

Automation

Unit of Production

Manufacturing

Supplies

Processes

Automation

Unit of Production

Manufacturing

Supplies

Processes
How do we securely get from here to there?
Possible roadmap for ecosystem security

Establish joint initiative vehicle to drive security
- Driven by participation across the value chain
- Business enablement for value-at-risk decisions

Establish governance framework
- Decision structures
- Collaboration enablers
- Operating processes

Deploy security integration architecture
- Foundation and distribution of trust
- Standard and interoperable identity schemes
- Identity resolution and mapping services
- Services for online security management

Alignment and compliance framework
- Measures of adoption and alignment
- Acceleration of lighthouse innovation
Iterative development of a security roadmap

Architecture Development Method

Cyber Security Framework

Security Profiles

Assets and Processes

Product Design

Process Design Plant Design

Engineering Commissioning

Operation

Service

Low

Medium

High

Extreme
Iterative development of a security roadmap

Security governance

Risk posture

Target

Review

Adjust

Threat intelligence

Security audits

Assets and Processes

Product Design

Process Design

Plant Design

Engineering Commissioning

Operation

Service

Security Profiles

Architecture

Development Method

Cyber Security Framework

Extreme

High

Medium

Low

Risk updates

Regulation updates

Standards updates

Risk posture

Threat intelligence

Security audits

Assets and Processes

Product Design

Process Design

Plant Design

Engineering Commissioning

Operation

Service

Security Profiles

Architecture

Development Method

Cyber Security Framework

Extreme

High

Medium

Low

Risk updates

Regulation updates

Standards updates

Target

Review

Adjust
Thank You.