Smart Manufacturing

General security and privacy principles to ensure a Trusted IoT environment
Industrial Security Incidents Effects

**No Effects**: 61%
- Production Downtime: 29%
- Threat to Production Systems: 14%
- Critical Loss of Know-How: 12%
- Loss of Quality: 4%
- Threat to Humans: 2%
- Threat to Environment: 0%

Security Standards known / applied
- BSI Baseline Protection: 48%
- IEC 62443: 45%
- ISO/IEC 27000: 40%
- VDI 2182: 32%

© VDMA 2013
Security and privacy risks

- **Production Downtime**
  - Illegal use of remote services
  - Infiltration of malicious code into machines

- **Loss of Know-how / IP**
  - Espionage
  - Social Engineering, Phishing
  - Intrusion into (connected) systems

- **Manipulation of Data**
  - Sabotage
  - Obfuscation of license violation

- **Statistics on customers or employees**
  - Unambiguous allocation of data
  - Collection / Aggregation of data
Security beyond market availability

“making available on the market”

Product
= Hardware
plus Software

Safety

Security

Manufacturer offers:
provide necessary updates to preserve the security level of the product

Use of the product …… and use …… and use …… and use ……

End of use
Security within (IoT) product lifecycles

<table>
<thead>
<tr>
<th>Security Level 1</th>
<th>Security Level 2</th>
<th>Security Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warranty period</td>
<td>Maintenance and service contract</td>
<td>Secure Development</td>
</tr>
</tbody>
</table>

Making available on the market
Audit / assessment
End of warranty period
End of use

Security recommendations

Requirements (customers, authorities)
Capabilities (products, services)

Steffen Zimmermann
Legislation
Business

VDMA
General recommendations for security and privacy in smart manufacturing

- Development of a general product security standard on at least European scale within CEN/ISO
  - Requirements of measures to implement in products and business
  - Goal: compatibility and comparability of products
- Implementation of a product security monitoring process in Europe
  - Interaction with business, consumers, authorities
  - Timely response to customer or third party notifications
  - Goal: Increasing awareness for security (by design)
- Implement security and privacy directive for IoT consumer products
  - Easy-to-understand security for uninformed end users
  - Transparency on data usage and collection
  - Goal: Increase product security transparency and create level playing field
- Leave Industrial IoT Security requirements open to standardisation and self declaration
  - Component lifecycle up to 20 years
  - High availability requirements
  - Non-patchable systems in critical sectors
General Principles to be applied to any IoT device (manufacturers view)

- Implement update mechanisms (if required)
- Document interfaces and data transmission
- Use secure protocols
- Secure remote maintenance
- Harden components and software
- Implement authentication features
- Use cryptography
- Train product developers on Security by Design
- Test security of both products and implementations
Guidance for „Industrie 4.0 Security“

- 85 recommendations
- 17 chapters
- **Target group**: manufacturing
- **Focus**: Products (plants, systems, machines, etc.)
  - Manufacturing / Operation of heterogeneous landscapes
  - Technical, organizational and administrative controls
  - Specific minimum requirements and responsibilities
  - Consideration of product lifecycle & updates
  - Practical feasibility and achievability

Available in German/English via
www.industrie40-security.de
Industrial Security

Steffen Zimmermann
Head of Competence Center Industrial Security
VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main - Germany

+49 69 6603 1978
Steffen.Zimmermann@vdma.org