

Atos

Trusted partner for your **Digital Journey**

DRAFT

No Industry 4.0 without Security

24-04-2017

1

Introduction to Atos and Industry 4.0

Who is Atos?

At a glance

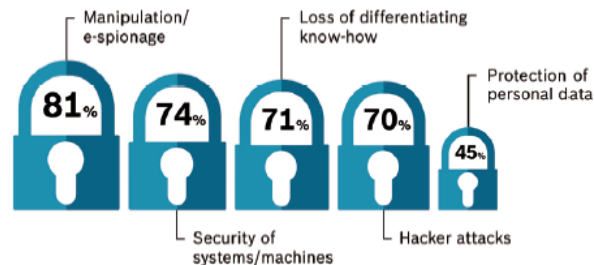


- #1 European in Hybrid Cloud
- #1 European in Big Data
- #1 European in Cybersecurity
- #1 European in High-Performance Computing
- #1 In terms of hosting and storage of European data

Surveys concerning Industry 4.0

Barriers for Industry 4.0

Data security; more than half of the participants expressed fundamental concerns

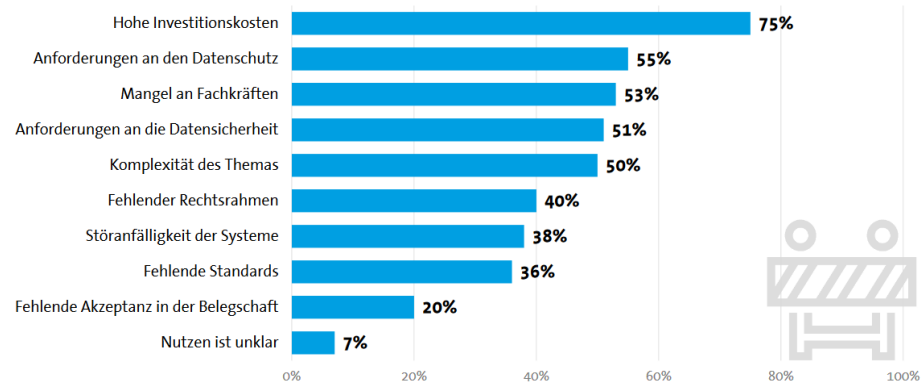


Source: Market study Bosch Software Innovations

High investment costs and concerns about data security and data protection are regarded to be problematic

Unternehmen fürchten hohe Anforderungen an Datenschutz

Welche Hemmnisse sehen Sie beim Einsatz von Industrie-4.0-Anwendungen in Ihrem Unternehmen?

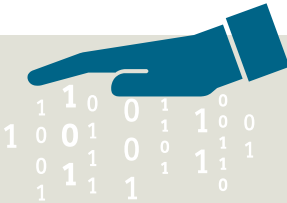


9 Basis: Industrieunternehmen ab 100 Mitarbeitern (n= 559) | Quelle: Bitkom Research

bitkom

The Challenge

IT versus OT security

IT Security		Industrial Security
<h3>Confidentiality</h3> <p>Integrity Availability</p>		<h3>Availability</h3> <p>Integrity Confidentiality</p>
Minutes are acceptable	Availability	Network disruptions < 300 ms
Network professionals	Installation	Plant personnel
Frequent audits, penetration tests, monitoring	Assessment	Audits, pentest and monitoring no common practice
Active protection mechanisms	Protection	Active protection mechanisms can shutdown operation
Common practice	Patching	Often not possible
Every 2-3 years	Investment cycle	Min. 10-20 years

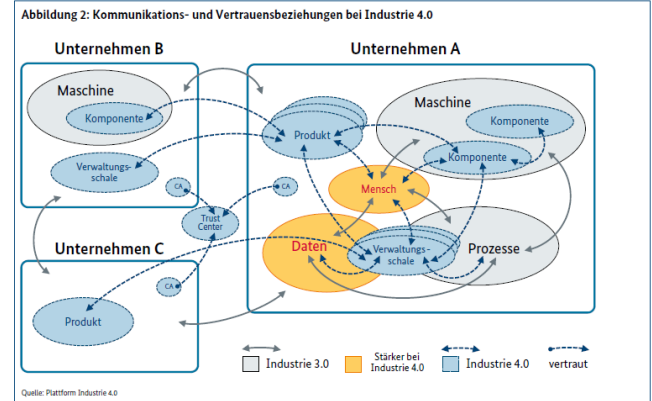
Developments and challenges for Industry 4.0

Developments

- ▶ **Dynamic networks**
 - value networks
 - further flexibility
 - interaction
- ▶ **Exchange of confidential data**
 - trustworthy relationships
- ▶ **Autonomous systems**
 - components making independent decisions

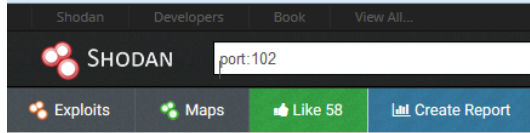
Challenges

- ▶ **Globally trusted relationships**
 - independent authority
 - standardized secure infrastructure
 - assessment methods for trustworthiness
- ▶ **Protection of intellectual property and personalized data**
 - secure and correct exchange of data
- ▶ **Allocated security**
 - security by design/development
 - holistic security
 - staged security
 - secure and trustworthy components

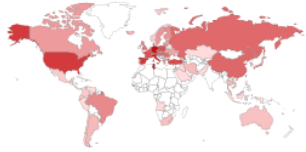


Hacking ICS devices is terribly easy

Step 1: Identify target



TOP COUNTRIES



Germany	223
Tunisia	222
Italy	201
Spain	112
United States	106

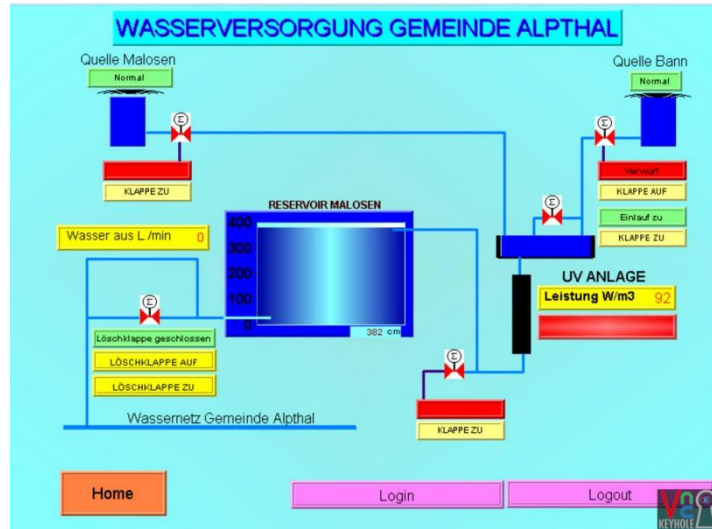
TOP ORGANIZATIONS

Deutsche Telekom AG	148
TOPNET	117
Tunisia BackBone	105
Telefonica de Espana	71
Telecom Italia	41

TOP PRODUCTS

Conpot	351
--------	-----

Step 2a: Access system: No password Set



Source: VNCKeyhole

Step 2a: Access system: Use default password

IoT Device Default Password Lookup

Check here if a default password is available for the IoT device:

SIMATIC|

Vendor: Siemens
Device: Simatic S7-300 (pre-2009 versions)
Default password: Hardcoded password: Basisk:Basisk
Port: 23/tcp, 80/tcp
Device type: PLC
Protocol: telnet, Http
Source: <http://www.wired.com/2011/08/siemens-hardcoded-password/>

Vendor: Siemens
Device: Simatic S7-1200 / S7-1500
Default password: admin:blank
Port: 80/tcp
Device type: PLC
Protocol: HTTP
Source: <https://www.dmcinfo.com/latest-thinking/blog/id/8567/siemens-s7-1200-web-server-tutorial-from-getting-started-to-html5-user-defined-pages>

Source: Defpass

2

Security Architecture for Industry 4.0

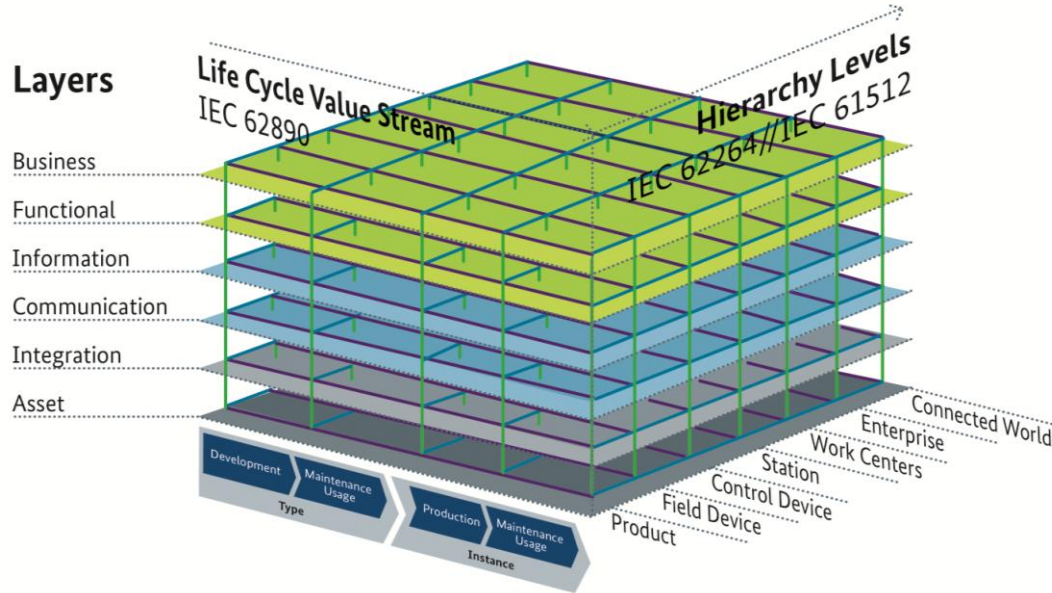
Reference architecture model for Industry 4.0 (RAMI) and security

Layers:

Security concerns all layers. Risks have to be assessed with a holistic approach

Value stream:

Security has to be assessed throughout the whole life cycle of the objects by the owner.

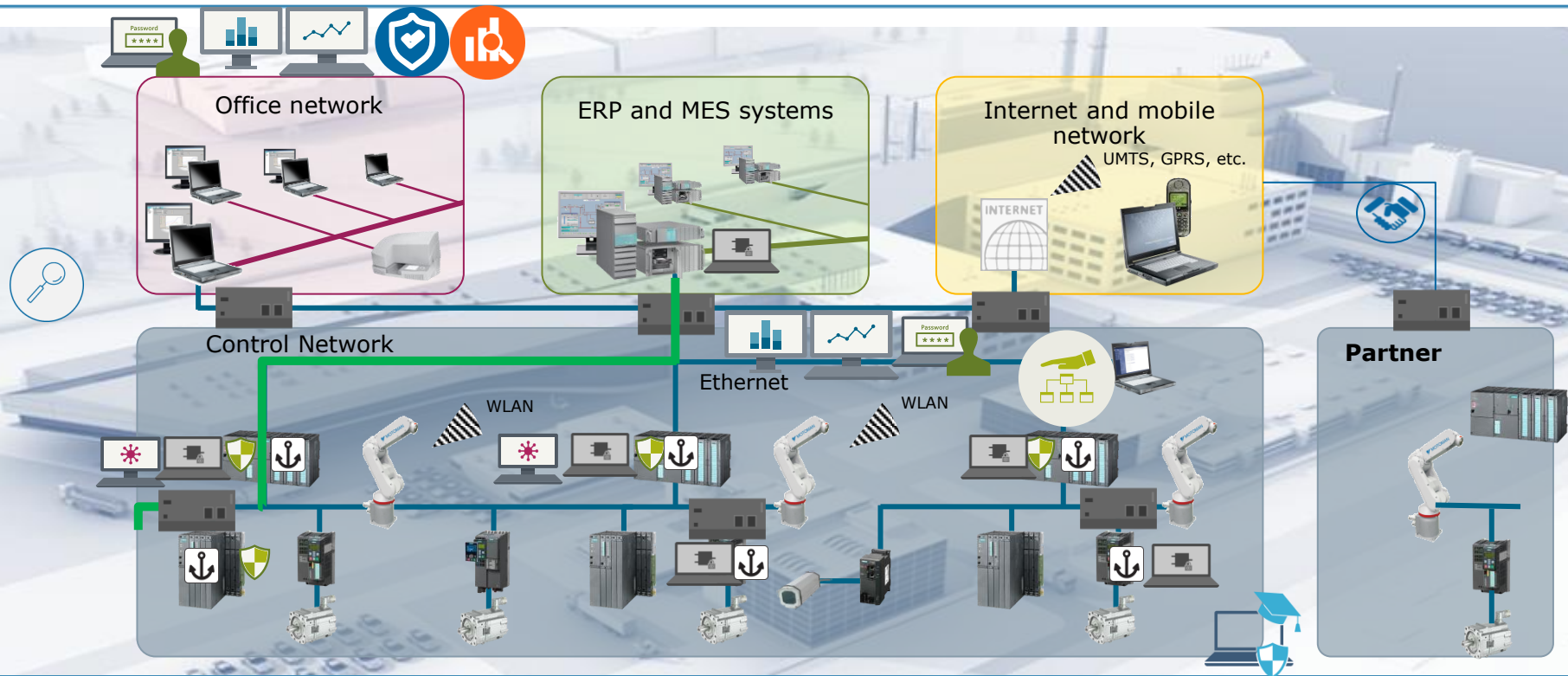


Hierarchy levels:

All objects and assets are subject to security analysis (risk analysis) and need to have security features matching their tasks and protection.

IT in industrial facilities

from communication islands to complex landscapes



3

Atos – Siemens
partnership

Atos and Siemens cooperation

Aligned cybersecurity portfolio to cover both IT and OT needs

Assess security

Evaluation of the current security status of an ICS environment

IT assessments by ATOS

- ISO/IEC 27001 security assessments
- Security maturity assessments
- Penetration tests & source code analysis
- ...

OT assessments by SIEMENS

- IEC 62443 assessment
- ISO 27001 assessment
- SIMATIC PCS 7 & WinCC assessment
- ...

Manage security

Comprehensive security through monitoring and proactive protection:

Monitor to detect indicators of compromise

Manage to keep security up-to-date

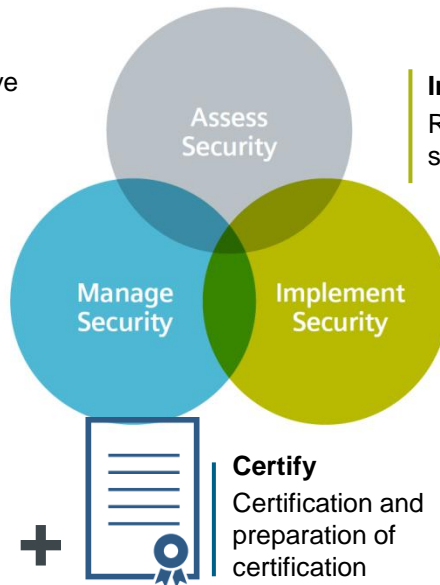
React fast to security-relevant threats

IT by ATOS

- Security monitoring
- Emergency response
- Network security
- ...

OT by Siemens

- Industrial security monitoring
- Remote incident handling
- Perimeter firewall management
- ...



Implement security

Risk mitigation through implementation of security measures for reactive protection

IT by ATOS

- Information security Management systems
- Security awareness
- Data protection
- ...

OT by SIEMENS

- Security awareness training
- Security policy and network consulting
- Perimeter firewall installation
- ...

Thanks

For more information please contact:
Winfried Holz

Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Unify, Yunano, Zero Email, Zero Email Certified and The Zero Email Company are registered trademarks of the Atos group. November 2016. © 2016 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

The Atos logo is displayed in white on a blue background. It features the word "Atos" in a bold, sans-serif font, with a stylized circular element integrated into the letter 'o'.