Secure Operations
Ensuring Cybersecurity to enable Industrial IoT
Leading global companies joined forces to encourage security in a networked world.

Charter of Trust

1. Protecting the data of individuals and companies
2. Preventing damage from people, companies and infrastructures
3. Establishing a reliable foundation on which confidence in a networked, digital world can take root and grow
Cybersecurity solutions focused on (OT) Security

### IT Security

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Asset lifecycle</th>
<th>OT Security</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5 years</td>
<td></td>
<td>20-40 years</td>
<td></td>
</tr>
<tr>
<td>Forced migration (e.g. PCs, smart phone)</td>
<td></td>
<td>Usage as long as spare parts available</td>
<td></td>
</tr>
<tr>
<td>High (&gt; 10 “agents” on office PCs)</td>
<td>Software lifecycle</td>
<td>Low (old systems w/o “free” performance)</td>
<td></td>
</tr>
<tr>
<td>Low (~2 generations, Windows 7 and 10)</td>
<td>Options to add security SW</td>
<td>High (from Windows 95 up to 10)</td>
<td></td>
</tr>
<tr>
<td>Standards based (agents &amp; forced patching)</td>
<td>Heterogeneity</td>
<td>Case and risk based</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main protection concept</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk vs Budget

Your Risk
Ever growing risk landscape

Your Budget
Wait or use your creativity
...costly impacts on operations

$1-2M / day
Economic impact of buying energy to replace energy production capabilities

$38-88M
Average annual spend on unplanned downtime

225,000
Customers without power due to Black Energy attack, 2015

$300M
Cost of NotPetya ransom ICS attack to single industrial company in 2017

Sources: 1) Richmond Times, 2) GEOilandGas, 3) E-ISAC, 4) CNBC
Structure by IEC 62443

1. General
   - 1-1: Terminology and concepts
   - 1-2: Master glossary
   - 1-3: System security compliance metrics
   - 1-4: IACS security lifecycle and use-case

2. Policy & Procedure
   - 2-1: Requirements for an IACS security management system
   - 2-2: Implementation guidance
   - 2-3: Patch management
   - 2-4: Installation & maintenance

3. System
   - 3-1: Security technologies for IACS
   - 3-2: Security levels for zones conduits
   - 3-3: System security requirements and levels

4. Component
   - 4-1: Product development requirements
   - 4-2: Technical security requirement for IACS components

Apply to Asset Owner
Apply to System Integrator
Apply to Component Supplier
IEC 62443 - Roles and Scope

Asset Owner
Operates and maintains

Service Provider

System Integrator
Designs and deploys

IACS environment / project specific

Product Supplier
Develops control systems
Develops components

Independent of IACS environment

Industrial Automation and Control System (IACS)

Operational policies and procedures
Maintenance policies and procedures

Automation solution

Basic Process Control System (BPCS)
Safety Instrumented System (SIS)
Complementary Hardware and Software

is the base for

Control System
Embedded devices
Network components
Host devices
Applications

is the base for
IEC 62443 - Roles and Scope
Cybersecurity Concepts for Mobility

Perimeter protection & IDS

…”installed base (legacy) and automation products without built-in cybersecurity”

Defense in Depth - IEC 62443

…”for future deployments, with products with built-in cybersecurity features”
Cybersecurity goal
IEC 62443 Security Levels

**SL 1**
Protection against unintentional or accidental attacks

**SL 2**
Protection against deliberate attacks with simple means
- Attacker type: Script Kiddie

**SL 3**
Protection against intentional attacks with advanced means
- Attacker type: Criminal organization

**SL 4**
Protection against intentional attacks with advanced resources
- Attacker type: Nations / Agencies
DCU
Data Capture Unit (Data Diode)
Enabling connectivity while keeping networks physically isolated? …Data Diode technology

- Guarantees protection and network isolation via hardware design that lacks the vulnerability of firewalls
- Reliable - MTBF +16yrs
- Galvanic isolation & physical separation ensures only one-way communication

Electromagnetic induction
Connectivity Concept

1. OT Network (SIG)
   - OWG
   - TVD
   - IXL
   - OCC

2. IT Network
   - Rail Operator
   - DCU
   - Router + FW
   - OWG
   - Cloud Connector
   - App
   - Storage
   - Connectors

3. Cloud
   - Vendor
   - Cloud App
   - Device Management
   - VPN

- Deploy Security Patches
  - Worldwide
- Rollout Applications and Updates
  - Worldwide
- Diagnostics and Local data storage
  - OWG receiver
- 0% risk of customer operation disruption
  - DCU
- Real-time data collection
  - OWG sender
Designed to be modular

1. OT Network (SIG)
   - OWG - Sender
   - SCADA / Interlocking

2. IT Network
   - Rail Operator
   - Router + FW
   - OWG - Receiver
   - DCU

3. Cloud
   - Vendor
     - Cloud App
     - Asset Management
   - VPN
USP's

Safety & Security

Safety assessment
SL3 - IEC 62443 4-2

0% risk
operation disruption

Vendor neutral
Standard protocols
IDS
Intrusion Detection System
**OSA**

**SIEM**
- Collect and aggregate security logs from HMI/Station/Server, industrial switch/router, firewall and OSA sensors
- Perform smart correlation and whitelist based analysis
- Provide security visualization for local OT admin

**Monitoring**
- Network traffic based asset detection and monitoring
- Anomaly detection
- Intrusion detection
- Malware traffic detection
- Forward security logs from endpoints in the same domain to OSA server

**Topologies**
- Asset Inventory
- Endpoint security log
- Syslog
- Network Sensor
  - Port mirror
  - Probing
- Industrial Switches

**Hardware**
- Server Hardware: 1U DELL R440
- Sensor Hardware: SIMATIC IPC427E
IT/Enterprise network

OT / Signaling (safety) network
What & Why

What

- JRS collects, stores and validates all critical SIG system data.
- JRS provides “Proof” that the stored data is unaltered and complete (integrity intact).
- JRS prevents the alteration and/or deletion of data acc. to IEC 62443 security concept:
  - Components
  - Communication

Why

- Data from juridical recorders is needed for all legal or formal investigations of accidents or “near-miss” situations.
- CENELEC 50701 will require data integrity tools for new railway systems.
Main features

1. **Modular juridical recorder** - Based on X.509 Certificates (PKI)

2. **RAID 6** - High performance and reliable of data storage

3. **Secure OS** – S2L2 with Certificates, Secure Boot and Whitelisting.

4. **IEC 62443 4-2 SL3** - Compliant

5. **Interference Free** – Compatible with DCU
Functionality

1 | Data collection
   DCU / Diagnostic PCs

2 | Data Storage
   RAID 6

3 | Evaluation & Validation
   JRS software

4 | Data Extraction
   Customer or Siemens
WORKING FOR A

POLLUTION-FREE TOMORROW

...ONE JOURNEY AT A TIME

SIEMENS

Mobility
Disclaimer

© Siemens AG 2020

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.
Contact

Published by Siemens Mobility GmbH

Andres G. Guilarte
Global Product Manager
SMO RI PR SD
Germany

E-mail andres.guilarte@siemens.com