Security in Automation –
possible threats and integrated measures in CODESYS

CODESYS Users Conference 2017
Manfred Werner
1. What is Security?

2. Situation in Industrial Security

3. Security Measures within CODESYS
What is Security?

**Safety**
- Protect humans
  - "Keep crazy people from doing stupid things"
- Restricted complexity
- Failure prediction
- Availability is not central

**Security**
- Protect investments
  - "Keep smart people from doing clever things"
- Constantly growing complexity
- Prediction of threat situation is not possible
- Availability has top priority
„Keep smart people from doing clever things!“
Vulnerabilities incidents in industrial security:

- RISI 2010 (ICSJWG Spring Conference):
  - 162 incidents since 2000
  - 78% unintended (handling or device errors, viruses)
  - 22% intentional, 53% of which by insiders (employees) and 47% by externals (including suppliers)

Vulnerabilities in products (ICS):

- ICS-Cert Advisories
  - 44 vulnerabilities in different products from January until May 2013
  - Are systematically searched for by security consultants (service providers)

Remarkable:
The incidents have nothing to do with the vulnerabilities.

Known, targeted attack on an application

- StuxNet
Vulnerabilities

Cloud / Fog Level

Production Hall
- Fieldbus interface
- Realtime communication between controllers
- Operation and monitoring
- Programming interface & remote maintenance

Engineering

Edge Controller

Remote Access

Automation Server

Machine 1

Machine 2

Machine 3

© 3S-Smart Software Solutions GmbH
IEC 62443 protection level

- **Level 1**: Occasional and accidental threat
  - Example: Hard disk failure
  - Example: Operating error

- **Level 2**: Intentional threat by simple means
  - Example: Password guessed correctly

- **Level 3**: Intentional threat by highly-developed means
  - Example: Hacker tools

- **Level 4**: Intentional threat by highly-developed means and extended resources
  - Example: Specific development
  - Example: Knowledge of the application
  - Example: Corruption of insiders
Security responsibilities in industrial control applications

- **Software Supplier**
  - Analyze assets and threats
  - Provide approved security measures
  - Provide technical documentation

- **Supplier of Automation devices**
  - Analyze assets and threats
  - Implement software and hardware security measures
  - Provide technical documentation

- **System Integrator / machine manufacturer**
  - Analyze assets and threats
  - Implement provided software and hardware security measures
  - Implement system security measures
  - Provide technical documentation

- **Plant operator / management**
  - Analyze assets and threats
  - Use available software, hardware and system security measures
  - Test / audit / certify system
  - Train staff
Security Whitepaper

- Guideline for OEMs, System Integrators and Operators
- Introduction in security subjects in industrial automation
  - Involved parties
  - Definition of the security level
  - Available tools in CODESYS to achieve the desired security level
  - Dealing with detected security vulnerability
# CODESYS Development System

## Security measures within CODESYS

<table>
<thead>
<tr>
<th>Measure</th>
<th>Whitepaper Section</th>
<th>Measure relevant for</th>
<th>Suitable measure against</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Suppliers of automation components</td>
<td></td>
</tr>
<tr>
<td>Encryption of the source code of the application</td>
<td>5.1.1 (10)</td>
<td>X</td>
<td>Occasional / unintentional threats and attacks</td>
</tr>
<tr>
<td>User administration on project level</td>
<td>5.1.2 (11)</td>
<td>X</td>
<td>Occasional / unintentional threats and attacks</td>
</tr>
</tbody>
</table>
CODESYS Security

Security measures within CODESYS

## CODESYS Runtime System

<table>
<thead>
<tr>
<th>Measure</th>
<th>Whitepaper Section</th>
<th>Measure relevant for</th>
<th>Suitable measure against</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Suppliers of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>automation components</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>System integrators / machine builders</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
<td></td>
</tr>
<tr>
<td>Access to the runtime system with authentication / permission management</td>
<td>5.2.1 (11)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encryption and signing of the executable application code</td>
<td>5.2.2 (11)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Controller operation mode</td>
<td>5.2.3 (12)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Interactive login</td>
<td>5.2.4 (12)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>5.2.5 (12)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Communication encryption between the IDE and the controller</td>
<td>5.2.6 (12)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
# IEC 61131-3 Application code

<table>
<thead>
<tr>
<th>Measure</th>
<th>Whitepaper Section</th>
<th>Measure relevant for</th>
<th>Suitable measure against</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Suppliers of automation components</td>
<td>System integrators / machine builders</td>
</tr>
<tr>
<td>Access restrictions out of the application / library</td>
<td>5.3.1 (13)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unlocking additional functions</td>
<td>5.3.2 (13)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
## CODESYS Visualization

<table>
<thead>
<tr>
<th>Measure</th>
<th>Whitepaper Section</th>
<th>Measure relevant for</th>
<th>Suitable measure against</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visualization User Management</td>
<td>5.4.1 (13)</td>
<td>Suppliers of automation components</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System integrators / machine builders</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Occasional / unintentional threats and attacks</td>
</tr>
<tr>
<td>Communication encryption for the CODESYS WebVisu</td>
<td>5.4.2 (13)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Attacks</td>
</tr>
</tbody>
</table>
Handling of security vulnerabilities in CODESYS

- External report
- OEM report
- Third party software
- Internal report

Creation of security Jira issue

- Decision fix version(s) / release date
- Assessment of impact, severity, tech. urgency
- Decision publishing date

- Fix
- Workaround
- Jira Security-Issues
- Version-No. Update recommendation
- Security-Patch
- OEM customer info „First-Advisory“
- Advisory Update (including Workaround)
- Release Advisory, Release Information Document

security@codesys.com
Thank you for your attention.