Challenges in Safety and Security for 
Industrial Automation Systems
Industrial Security (IEC 62443)


Martin Zappe
Business Unit Manager
Industrial Engineering

Udo Hipp
Head of Functional Safety and Agile Engineering
BC Industrial Safety & Security

Abstract

- In April 2016 the BSI (Federal Office for Information Security) released a study about the security status of OPC UA protocol. The performed analyzes showed, that OPC UA offers a good security level. In this context it is important to understand, that the OPC UA specification can specify IT-security-measures which secure the related communication only. Threads which attack e.g. the operating system have to be secured separately. Hence the engineer needs a bouquet of balanced measures for securing his system/application. These facts lead us to the "Challenges in Safety and Security for industrial Automation Systems" - in this session we will describe an all-embracing engineering approach which incorporates also the system view by the application of IEC 62443.
Agenda

- ICS AG – Profile
- OPC UA
  - Basics
  - Level of Security
  - Security Measures
- About IEC 62443
  - Basic Principles
  - Foundational Requirements
- Risk Assessment
- Recap
ICS AG – Profile

- **Facts**
  - formation 1966 – more than 50 years
  - privately owned – no investors
  - registered capital 2.65 Mio EUR

- **Profile**
  - We are an international Systems- and Software Engineering Company
  - ICS AG’s responsiveness to customer needs and its innovative competence centers ensure your success
  - Our employees are a key asset. Most have been with us for many years
  - We are distinguished by a reputation for premium engineering and support quality focused on: safety critical, mission critical, business critical Applications

Review – ROS & OPC UA Basics

- **Review - ROS Industrial Day 2016**
  - “A Status Update”, Mr. M. Keinert, isw.uni.stuttgart.de [MK]
  - „Advanced robotics …“, Mr. B. Gerkey, ROS Foundation [BG]

- **ROS based on OPC UA for seamless Integration** [MK]
  - Platform and manufacturer independent communication

- **Making ROS relevant for Industry 4.0** [MK]
  - OPC UA is a key technology in the context of Industry 4.0
  - ROS 2.0 enables the integration of the OPC UA communication technology

- **„Classic“ ROS ist not secure** [MK]
  - Front Door is wide open (no authentication, no encryption …)
  - ROS assumes a secure network

- **Process level security** [MK]
OPC UA – Level of Security

- OPC UA Security Analysis Study
  - Commissioned by the Federal Office for Information Security (BSI)
  - Published 02 / 03 / 2017
  - Method: STRIDE

- Analysis were performed
  - In the first part of the project, the specification of the OPC UA was analyzed Protocol version 1.02 on systematic errors. This analysis was divided into the following steps:
    - Threat analysis (analysis of the objectives and threats, analysis of threats and measures)
    - Analysis of the OPC UA specification in detail with an emphasis on the parts of 2, 4, 6, 7 and 12

- Analysis Conclusion and Result
  - If confidential data is exchanged „securityMode SignAndEncrypt“ is mandatory.
  - OPC UA offers a high level of Security
  - If „securityMode Sign“ and „securityMode SignAndEncrypt“ is used OPC UA offers a high level of Security

OPC UA – Security Measures

- OPC Foundation Security working group
  - Assessed the findings in the BSI report and initiated necessary measures
  - No major flaws had been detected,
  - Measures defined will help to improve the OPC UA Specification and the implementations.

- OPC UA Security Architecture – „Castle Approach“
  - Defense in Depth
IEC 62443 and OPC UA - „Castle Approach“ (Defense-in-Depth)

OPC UA – Security Architecture
OPC UA – Security Architecture

Industrial Security – Standards and Guidelines

Fulfillment of Standing Orders

<table>
<thead>
<tr>
<th>Applicable Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 62443:</td>
</tr>
<tr>
<td>Industrielle Kommunikationssysteme – IT-Sicherheit für Netz und Systeme</td>
</tr>
<tr>
<td>ISO 27001:</td>
</tr>
<tr>
<td>IT-Sicherheitsverfahren – Informationssicherheits- Managementsysteme – Anforderungen</td>
</tr>
</tbody>
</table>

Guidelines

<table>
<thead>
<tr>
<th>[NIST SP 800-30 R1]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guide for Conducting Risk Assessments – Information Security</td>
</tr>
<tr>
<td>[VDI VDI 2182]:</td>
</tr>
<tr>
<td>IT-sicherheit für industrielle automation - example of use of the general model for device manufacturer in factory automation</td>
</tr>
<tr>
<td>[BSI IT-Grundwissen] Catalogue:</td>
</tr>
<tr>
<td>Leitfaden zur Umsetzung der ISO 27000 Reihe</td>
</tr>
</tbody>
</table>
Industrial Security – Documented Evidence of Conformity

ISO 27000ff
- Installation, Implementation, Operation and continuous optimization of ISMS

VDI/VDE 2182
- "IT-security for industrial automation - example of use of the general model for device manufacturer in factory automation" Inspection according to VDI 1000 - content is transferred into IEC 62443

IEC 62443
- IT-Security für Industrial Automation and Control Systems

Overview - IEC 62443

General
- 1.1 Concept and Models
- 1.2 Master glossary of terms and abbreviations
- 1.3 System security, conformance metrics
- 1.4 IACS security life-cycle and use cases

Policies & Procedures
- 2.1 Requirements for an IACS security management system
- 2.2 Implementation guidance for an IACS security management system
- 2.3 Patch management in the IACS environment
- 2.4 Requirements for IACS station supplier
Overview - IEC 62443

General

Informative
superordinate Aspects, Terminology, Metrics

Policies & Procedures

Req. SMS
ISO 27001/2 profile

Requirements
Service Provider

System

3.1 Security technologies in IACS
3.2 Security risk assessment and system design
3.3 System security requirements and security levels

Component

6.1 Project development requirements
4.2 Technical security requirements for IACS components

Quelle: ISA99 Committee abgerufen am 20.01.2016
Overview - IEC 62443

Requirements
Asset Owner/System Integrator
Zones/Conduits, Segmentation, Risk Analysis/-level

Requirements
Component Supplier
IT-Security as mandated asset of Dev.-Processes

Main Objective:
- reduce effort!
- hence Risk Analysis is essential

Coherence – IEC 62443

Asset Owner

System Integrator

Product supplier

Risk Analysis

Industrial Automation /控制系统 (IEC 62443-2-4)
Operation and Maintenance (Processes)

System

Subsystem 1
Subsystem 2
Additional HW und SW

OPC UA - Security Architecture

Application
Embedded System
Network- Component
Platform- Component

OPC UA

Product
(IEC 62443-4-2)

System, Sub-System or Component, e.g.:
OPC UA – Security Architecture

© Hipp/Zappe

© Hipp/Zappe

OPC UA – Security Architecture

- Data Flow
- Authentication
- Use Control
- Timely Response
- Availability

Security Architecture

- Basic principles
- People
- Process
- Technology

IEC 62443 - Basic Principles

People
Process
Technology

Source: outfit4events.de
Source: opcfoundation.org

People, Process, Technology, Security, Management, Verification, Validation, Support, Availability

Source: ISA-62443-1-1
Vector of Security Levels - IEC 62443

- Usage of a Vector of Security Levels
  - inherits SEVEN Foundational Requirements (FR)
  - instead of a single protection factor

- Vector of Security Levels allows definable separations between Security Levels for the different FRs using language

<table>
<thead>
<tr>
<th>Foundational Requirements</th>
<th>FRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification, Authentication and Access Control (IAC)</td>
<td>SEVEN</td>
</tr>
<tr>
<td>Use Control (UC)</td>
<td></td>
</tr>
<tr>
<td>System Integrity (SI)</td>
<td></td>
</tr>
<tr>
<td>Data Confidentiality (DC)</td>
<td></td>
</tr>
<tr>
<td>Restricted Data Flow (RDF)</td>
<td></td>
</tr>
<tr>
<td>Time Response To Events (TRE)</td>
<td></td>
</tr>
<tr>
<td>Resource Availability (RA)</td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity risk assessment based on 62443-2

- Challenges:
  - Identify Threats and Vulnerabilities
  - Identify the needed security requirements
  - Manual effort for security risk analysis on component level
Threats and Vulnerabilities database sources

- **Common Attack Pattern Enumeration and Classification (CAPEC):**
  - The CAPEC database documents attack patterns using a unique id, describes the weakness (CWE-ID), likelihood, consequences in terms of Confidentiality, Integrity, Availability (16.08.2017: 206 entries)

- **Common Vulnerabilities and Exposures (CVE):**
  - The CVE database documents vulnerability of products and software using a unique id. (16.08.2017: 89118 entries)

- **Common Weakness Enumeration (CWE):**
  - The CWE database documents weaknesses of products and software using a unique id, countermeasures and attack patterns enabled by this weakness. (16.08.2017: 705 entries)
CAPEC: Threats and Vulnerabilities database sources

Common Attack Pattern Enumeration and Classification - https://capec.mitre.org/

Some Well-Known Attack Patterns:
- HTTP Response Splitting (CAPEC-34)
- Session Fixation (CAPEC-61)
- Cross Site Request Forgery (CAPEC-62)
- SQL Injection (CAPEC-66)
- Cross-Site Scripting (CAPEC-63)
- Buffer Overflow (CAPEC-100)
- Clickjacking (CAPEC-103)
- Relative Path Traversal (CAPEC-139)
- XML Attribute Blowup (CAPEC-229)

CVE: Threats and Vulnerabilities database sources

Common Vulnerabilities and Exposures - https://cve.mitre.org/

<table>
<thead>
<tr>
<th>Date</th>
<th>Number</th>
<th>Title</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-07-31</td>
<td>CVE-2017-12070</td>
<td>Security Update for OPC UA .NET Sample Applications</td>
<td>4.9 (medium)</td>
</tr>
<tr>
<td>2017-07-31</td>
<td>CVE-2017-12083</td>
<td>Security Update for the OPC UA .NET Sample Code</td>
<td>8.2 (high)</td>
</tr>
<tr>
<td>2017-07-28</td>
<td>CVE-2017-11672</td>
<td>Security Update for Local Discovery Services (LDS)</td>
<td>4.4 (medium)</td>
</tr>
<tr>
<td>2017-12-09</td>
<td>CVE-2017-17451</td>
<td>Security Update for Local Discovery Services (LDS)</td>
<td>4.4 (medium)</td>
</tr>
</tbody>
</table>

Source: https://opcfoundation-videnapplications.org/files/technicalbulletines/
Threats and Vulnerabilities database sources

Common Weakness Enumeration - https://cwe.mitre.org/

<table>
<thead>
<tr>
<th>Rank</th>
<th>Score</th>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>93.0</td>
<td>CWE-99</td>
<td>Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')</td>
</tr>
<tr>
<td>2</td>
<td>83.3</td>
<td>CWE-76</td>
<td>Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')</td>
</tr>
<tr>
<td>3</td>
<td>79.0</td>
<td>CWE-120</td>
<td>Buffer Copy without Checking Size of Input ('Classic Buffer Overrun')</td>
</tr>
<tr>
<td>4</td>
<td>77.7</td>
<td>CWE-79</td>
<td>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</td>
</tr>
<tr>
<td>5</td>
<td>76.9</td>
<td>CVE-904</td>
<td>Missing Authorization for Critical Function</td>
</tr>
<tr>
<td>6</td>
<td>76.8</td>
<td>CWE-862</td>
<td>Missing Authorization</td>
</tr>
<tr>
<td>7</td>
<td>75.0</td>
<td>CWE-78</td>
<td>Use of Hard-coded Credentials</td>
</tr>
<tr>
<td>8</td>
<td>75.0</td>
<td>CVE-311</td>
<td>Missing Encryption of Sensitive Data</td>
</tr>
<tr>
<td>9</td>
<td>74.0</td>
<td>CWE-414</td>
<td>Unrestricted Upload of File with Dangerous Type</td>
</tr>
<tr>
<td>10</td>
<td>73.8</td>
<td>CVE-807</td>
<td>Reliance on Untrusted Inputs in a Security Decision</td>
</tr>
</tbody>
</table>

Using Threats and Vulnerabilities database sources

Challenge is the definition of a threat model that can be used in cyber security risk assessment to overcome:
- Cyclic and timely update of databases
- Large amount of entries
- Linkage between CAPEC, CWE and CVE ids using a multiple relationship
Using Threats and Vulnerabilities database sources

Proposed solution:

1. Identify threats
2. Identify vulnerabilities
3. Identify consequences and impact
4. Determine unmitigated likelihood
5. Calculate unmitigated cybersecurity risk
6. Determine Security level target
7. Derivation security requirements
8. Identify and evaluate existing countermeasures
9. Reevaluate likelihood and impact
10. Determine residual risk
11. Compare residual risk with tolerable risk
12. Apply additional cybersecurity countermeasures
13. Filter criteria

Most databases (CAPEC, CWE, CVE) and the common understanding of security challenges are working with the three basic values Confidentiality, Integrity, Availability

The security requirements of 62443 are grouped in seven Foundational Requirements

Proposed solution: Mapping of CIA to foundational requirement

<table>
<thead>
<tr>
<th>CIA / Foundational Requirements</th>
<th>IAC Identification and Authentication Control</th>
<th>UC Use Control</th>
<th>SI System integrity</th>
<th>DC Data confidentiality</th>
<th>RDF Restricted Data Flow</th>
<th>TRE Timely response to events</th>
<th>RA Resource Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Integrity</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identify security requirements in the scope of 62443

- Common databases:
  No relationship between Security Requirements and the required Security Level

- In 62443-3-3 security requirements are allocated to the security level (determined in the security risk analyse)

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Definition of Security level</th>
<th>Identification and authentication (IAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SL 0</td>
<td>No specific requirements or security protection necessary</td>
<td>None</td>
</tr>
<tr>
<td>SL 1</td>
<td>Protection against casual or coincidental violation</td>
<td>SR 1.1 Identification and authentication of human users</td>
</tr>
<tr>
<td>SL 2</td>
<td>Protection against intentional violation using simple means with low resources, genetic skills and moderate motivation</td>
<td>additionally: SR 1.1 RE 1 (from SL 2) Unique identification and authentication, SR 1.2 (from SL 2) Identification and authentication of software processes and devices</td>
</tr>
<tr>
<td>SL 3</td>
<td>Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation</td>
<td>additionally: SR 1.1 RE 1 (from SL 3) Multifactor authentication, SR 1.2 RE 1 (from SL 3) Uniform user account management</td>
</tr>
<tr>
<td>SL 4</td>
<td>Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation</td>
<td>additionally: SR 1.1 RE 1 (from SL 4) Multifactor identification and authentication across all networks</td>
</tr>
</tbody>
</table>

Manual effort for security risk analyzes on component level

- System definition, high level risk assessment and the partition of the system into zones and conduits are manual tasks on system and security Expert level
- The detailed cyber security risk assessment on every component is a timeconsuming error-prone task

Proposed solution:
- Use a formalized description of the system definition
- Use a tool generated threat model (CAPEC, CWE, CVE)
- Use a tool generated assignment of threats to components based on the formalized system definition
- Use consequences and impact based on CIA of the threat model
- Define a basic relationship between threat and security requirements of the 62443
- Calculate automatically the intermediate residual risk values
- Focus the individual security expertise on identification of vulnerabilities and the definition of additional cyber security countermeasures
Recap

- Industrial Security matters!
- Conscious Mind Set and Process is essential!
- ROS should support Vulnerability data bases!
- Risk Assessment reduces overall effort – IEC 62443!

Thank you, for your Attention!
Recap

Industrial Security is the matter of the Management!
Establish a Security Officer – implement an ISMS!
Secure Products mandate an ISMS

Standards are a good starting point – support of experts is helpful
Every Branch/Industry needs an individual interpretation/adaptation

ISO 27000ff and IEC 62443 valuable standards!