
Katrin Neubauer, Rudolf Hackenberg

Katrin Neubauer
Dept. Computer Science and Mathematics
Ostbayerische Technische Hochschule Regensburg, Germany
katrin1.neubauer@oth-regensburg.de
Katrin Neubauer

Education:

Since 02/2014  PhD Student (Applied Informatics)
Georg-August University Göttingen (Germany)

03/2012 – 09/2013  Master (M.Sc.) Applied Research in Engineering Sciences
University of Applied Sciences Regensburg (Germany)

10/2008 – 03/2012  Bachelor (B.Sc.) Medical Information Technology
University of Applied Sciences Regensburg (Germany)

Work Experience:

Since 01/2016  Research Assistant
University of Applied Sciences Regensburg (Germany)

R-Tech GmbH, Regensburg (Germany)

04/2012 – 08/2013  Research Assistant
R-Tech GmbH, Regensburg (Germany)
Outline
1. Motivation – Smart Grid – Cyber Physical Systems
2. Security assessment of Cyber Physical Systems
4. Application example
5. Summary
1. Motivation

Smart Grid

producers

consumer

customer

...

EVU communication platform

Smart Meter Gateway

energy
(smart metering, feed-in management, ...)

Smart Home
(intelligent household devices)

gas
(current consumption data, ...)

water
(current consumption data, ...)

value-added-service
(eHealth, ...)

10/7/2020
Smart Grid – Cyber Physical Systems

- Cyber Physical Systems (CPS) – characteristics of future systems (Smart Grid)
- High scalable
  - Use case: data logging “electricity”
  - Data flaw: final consumers – energy supplier
  - 2 million participants – 192 million consumption values per day
- Volatile
  - Transfer of data every 15 min -> communication
- High data volume
  - 2 million participants – 22 gigabyte data
- Different types of data
  - Customer data, power consumption, IP address
2. Security assessment of CPS

• Security assessment of CPS based on previous models not possible!
  • Consideration of business process
  • Consideration of development process
  • Consideration of sub-process
• Open: Security assessment of CPS
  • Data security according to the requirements of CPS
  • Consideration: entire process
• Development goal: process-oriented procedure for security assessment of CPS
 Requirement criteria for security assessment of CPS

- Data security
- Scalability
- Real-time
- Performance
- Functional safety
- Volatility

- Security assessment of CPS must be developed according to this requirement criteria

- In the first step, the following requirement criteria are focused:
  - Data security (DS)
  - Scalability (SC)
  - Real-time (RT)
- Assessment of the Use Case
  - UseCase\textsubscript{process} = (DS, SC, RT)
  - Security assessment results from the description of the process
- Approach
  - Analysis
    - Process and infrastructure
    - Data an information
  - Security Assessment UseCase\textsubscript{process} = (DS, SC, RT)
  - Automated mapping of model based on the use case process and assignment of security measures

Requirement criteria CPS

Data security

1. Category: non sensitive data
   • All data that do not contain any personal reference or have been made anonymous
   • The security level is low

2. Category: high sensitive data I
   • All data which, through the combination of several data in category 2 and 3, have a personal reference, but do not have a direct reference themselves
   • The security level is minimal

3. Category: high sensitive data II
   • All data which, through the combination of a further date in categories 2 and 3, have a personal reference, but do not have a direct reference themselves
   • The security level is intermediate

4. Category: high sensitive data III (personal data)
   • All data that are personal data or data worth protecting according to the Federal Data Protection Act
   • The security level is high

<table>
<thead>
<tr>
<th>category</th>
<th>description</th>
<th>security level</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Category</td>
<td>non sensitive data</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>2. Category</td>
<td>high sensitive data I</td>
<td>minimal</td>
<td>1</td>
</tr>
<tr>
<td>3. Category</td>
<td>high sensitive data II</td>
<td>intermediate</td>
<td>2</td>
</tr>
<tr>
<td>4. Category</td>
<td>high sensitive data III</td>
<td>high</td>
<td>3</td>
</tr>
</tbody>
</table>

Requirement criteria CPS

Scalability
• number of participating participants.
• Participants: users and devices
  • $\leq 1$
  • $2 \leq 100$
  • $101 \leq 10.000$
  • $\geq 10.001$

Real-Time
• System response time
  • $\leq 1$ sec
  • $2$ sec $\geq 1$ min
  • $1$ min $\geq 15$ min
  • $\geq 15$ min

<table>
<thead>
<tr>
<th>description</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\leq 1$</td>
<td>0</td>
</tr>
<tr>
<td>$2 \leq 100$</td>
<td>1</td>
</tr>
<tr>
<td>$101 \leq 10.000$</td>
<td>2</td>
</tr>
<tr>
<td>$\geq 10.001$</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>description</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\leq 1$ sec</td>
<td>0</td>
</tr>
<tr>
<td>$2$ sec $\geq 1$ min</td>
<td>1</td>
</tr>
<tr>
<td>$1$ min $\geq 15$ min</td>
<td>2</td>
</tr>
<tr>
<td>$\geq 15$ min</td>
<td>3</td>
</tr>
</tbody>
</table>
4. Application example

- **SEGAL**
  - Use case of Smart Grid
  - Value-added services
  - Ambient Assisted Living (AAL-services)

- Which process exists?
  - **Process 1: Initialize device**
  - Process 2: Delete device
  - Process 3: Update
  - Process 4: Transmit data
  - **Process 5: Transmit emergency data**
4. Application example

SEGAL: process 1 – initialize device

Data Security

<table>
<thead>
<tr>
<th>category</th>
<th>description</th>
<th>security level</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Category</td>
<td>high sensitive data II</td>
<td>intermediate</td>
<td>2</td>
</tr>
</tbody>
</table>

Scalability

<table>
<thead>
<tr>
<th>description</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 ≤ 100</td>
<td>1</td>
</tr>
</tbody>
</table>

Real time

<table>
<thead>
<tr>
<th>description</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 min ≥ 15 min</td>
<td>2</td>
</tr>
</tbody>
</table>

-> Process\text{ID} = (2,1,2)
SEGAL: process 2 - transmit emergency data

Data Security

<table>
<thead>
<tr>
<th>category</th>
<th>description</th>
<th>security level</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>high sensitive data II</td>
<td>intermediate</td>
<td>2</td>
</tr>
</tbody>
</table>

Scalability

<table>
<thead>
<tr>
<th>description</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 ≤ 100</td>
<td>1</td>
</tr>
</tbody>
</table>

Real time

<table>
<thead>
<tr>
<th>description</th>
<th>coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 1 sec</td>
<td>0</td>
</tr>
</tbody>
</table>

$\Rightarrow \text{Process}_{TED} = (2, 1, 0)$
4. Application example

Security assessment of SEGAL

Next Step:
Definition security measures
- Which authentication methods are suitable for the process (use case)?
5. Summary

New framework for security assessment: process-oriented procedure for security assessment of CPS

• Approach
  • Analysis
    • Process and infrastructure
    • Data and information
  • Security Assessment UseCase\text{process} = (DS, SC, RT)
  • Automated mapping of the trust model based on the UseCase process and assignment of security measures

Next steps
  • Automatization of the framework
  • Definition of the security measures