OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems

Katrin Neubauer, Rudolf Hackenberg

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

IARIA

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)

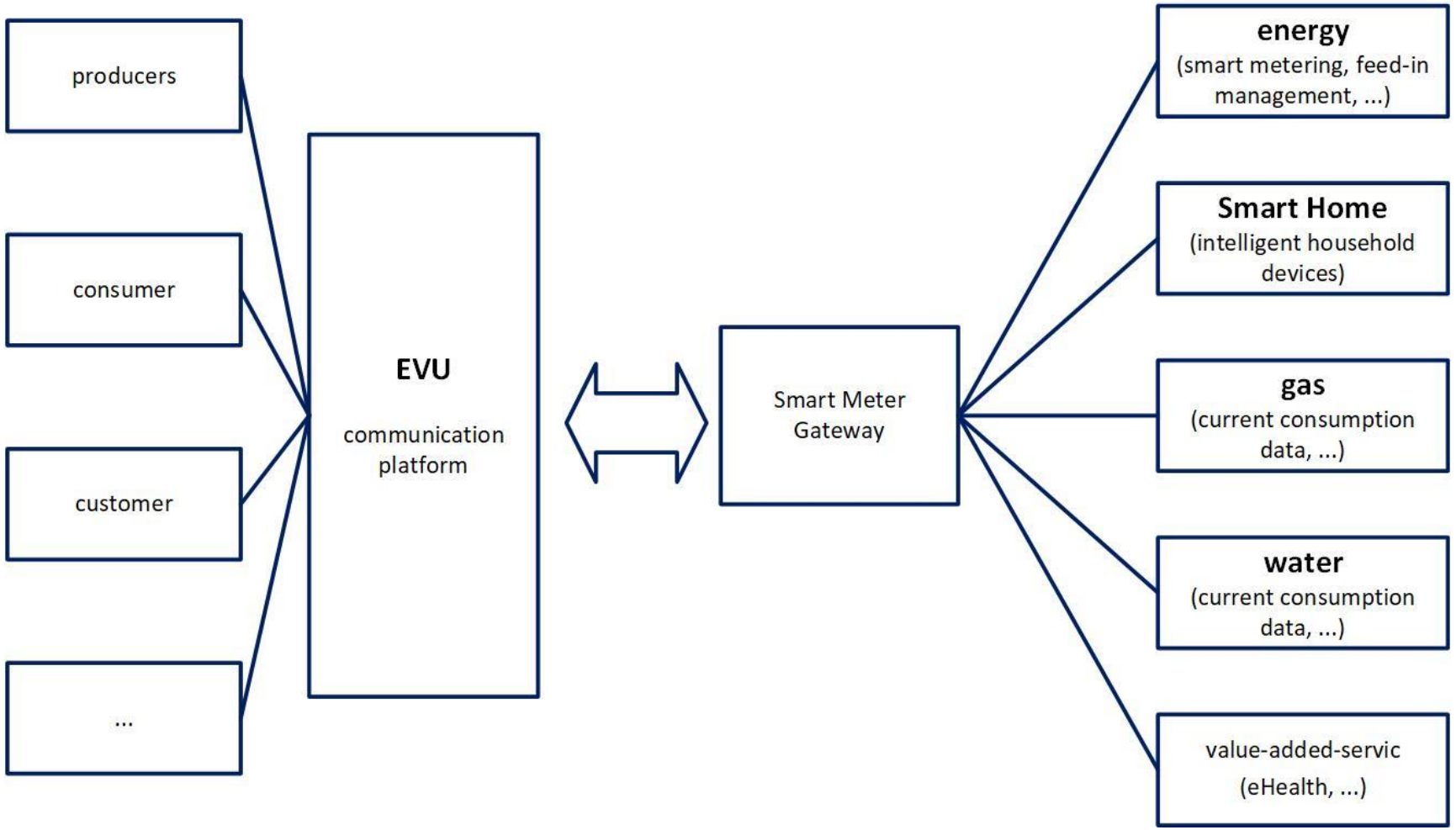
Work Experience:

Since 01/2016	**Research Assistant** University of Applied Sciences Regensburg (Germany)
09/2013 – 12/2015	**Project Manager “Information Security for small and medium-sized enterprises”** 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
3. Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems
4. Application example
5. Summary

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-servic
(eHealth, ...)

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

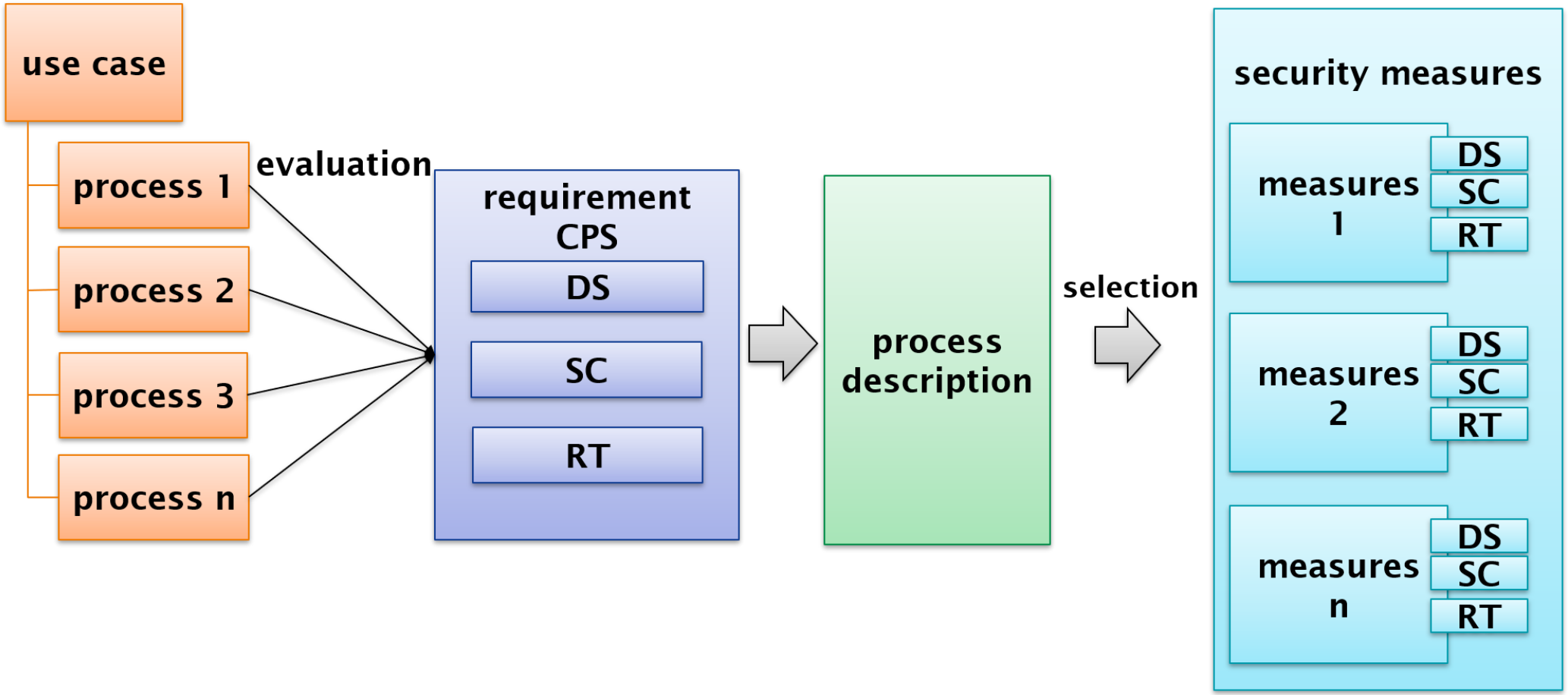
- Data security
- Scalability
- Real-time
- Performance
- Functional safety
- Volatility

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

3. Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems

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

3. Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems



Requirement criteria CPS

DS

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

category	description	security level	coding
1. Category	non sensitive data	low	0
2. Category	high sensitive data I	minimal	1
3. Category	high sensitive data II	intermediate	2
4. Category	high sensitive data III	high	3

Requirement criteria CPS

Scalability

- number of participating participants.
- Participants: users and devices
  - ≤ 1
  - 2 ≤ 100
  - 101 ≤ 10.000
  - ≥ 10.001

SC

description	coding
≤ 1	0
2 ≤ 100	1
101 ≤ 10.000	2
≥ 10.001	3

Real-Time

- System response time
  - ≤ 1 sec
  - 2 sec ≥ 1 min
  - 1 min ≥ 15 min
  - ≥ 15 min

RT

description	coding
≤ 1 sec	0
2 sec ≥ 1 min	1
1 min ≥ 15 min	2
≥ 15 min	3

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**

SEGAL: process 1 – initialize device

Data Security

category	description	security level	coding
3. Category	high sensitive data II	intermediate	2

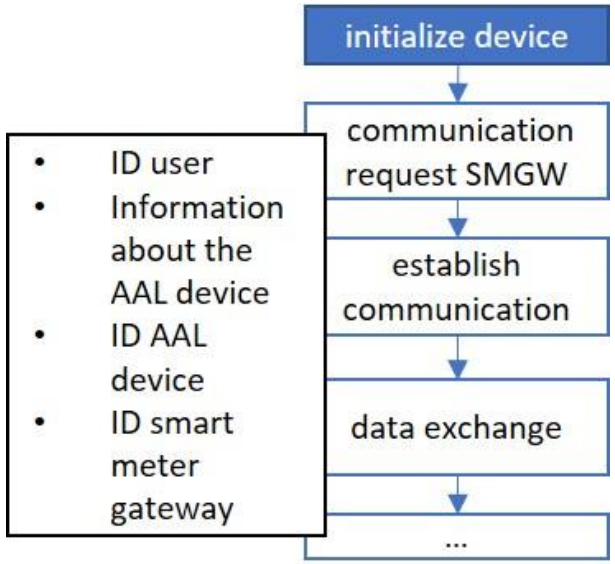
Scalability

description	coding
$2 \leq 100$	1

Real time

description	coding
1 min $\geq$ 15 min	2

-> $Process_{ID}$ = (2,1,2)



SEGAL: process 2 – transmit emergency data

Data Security

category	description	security level	coding
3. Category	high sensitive data II	intermediate	2

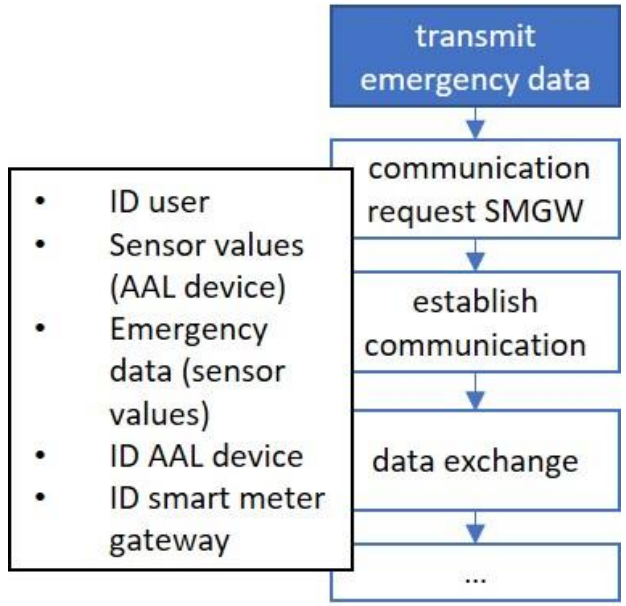
Scalability

description	coding
$2 \leq 100$	1

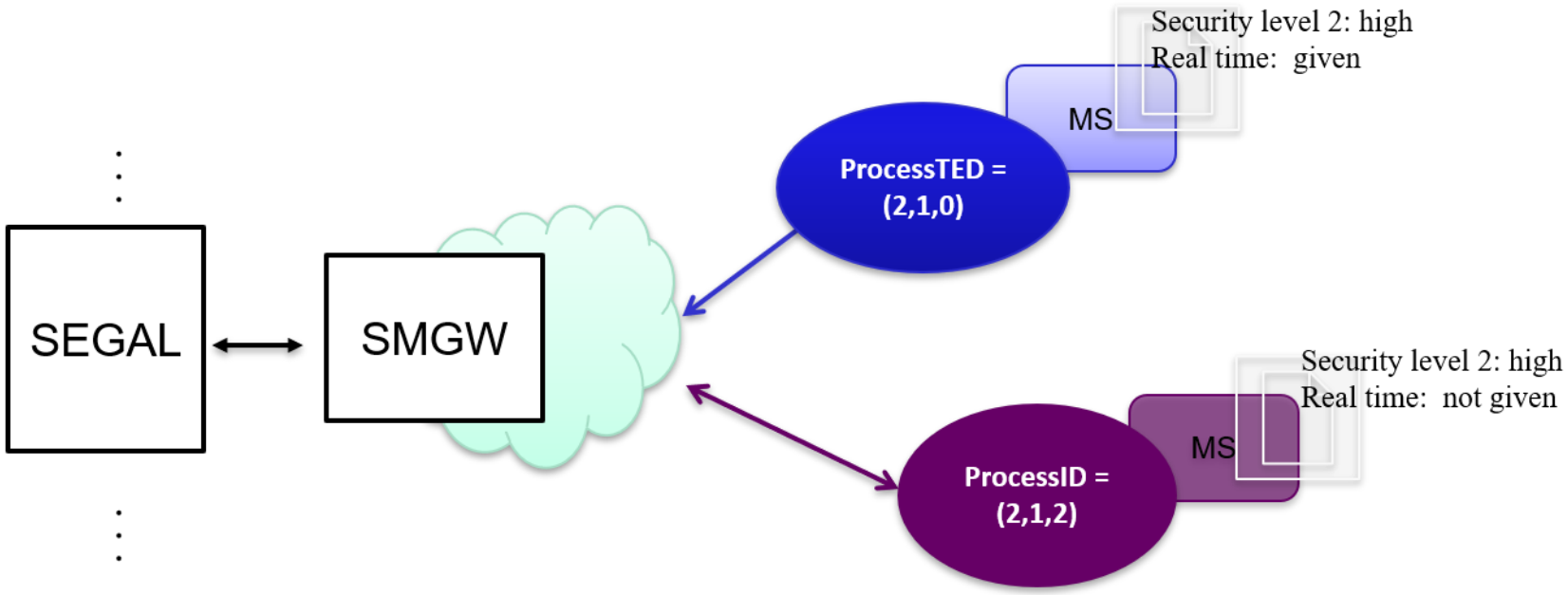
Real time

description	coding
≤ 1 sec	0

-> $Process_{TED} = (2,1,0)$



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 $\text{UseCase}_{\text{process}}$ = (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

Katrin Neubauer
katrin1.neubauer@oth-regensburg.de