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

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

Rudolf Hackenberg
Dept. Computer Science and Mathematics
Ostbayerische Technische Hochschule
Regensburg, Germany
email: rudolf.hackenberg@oth-regensburg.de

***Abstract*—Cloud Computing and Internet of Things (IoT) influence the constantly growing networking of systems. Both belong to Cyber Physical Systems (CPS) are highly networked systems. The increasing establishment of CPS creates new challenges and further security and data protection aspects arise. Existing frameworks for security assessment are not suitable for CPS. The requirement criteria for CPS are scalability, real-time, performance, functional safety and volatility. Data security has so far been evaluated by the two-level trust model (secure and insecure). This trust model is not suitable for CPS. The reasons for this are the large amount of data and the wide variety of data types. This paper presents the required criteria for security assessment of CPS, the development of the Process-oriented Framework for Security Assessment of Cyber Physical Systems and the application of the security model. The Process-oriented Framework for Security Assessment of Cyber Physical Systems includes the steps analysis of the application, security, scalability and real-time assessment and automated mapping of security measures.**

Keywords*—*Cyber Physical System; security assessment; security analysis; Internet of Things; Smart Grid.

I. Introduction

Cyber Physical Systems (CPS) are the next generation of engineered systems. Cloud Computing and Internet of Things (IoT) have an impact on networking in industrial environments and daily life. The digital age is influenced by SMAC technologies. Social, mobile, analytics and Cloud Computing are the SMAC technologies. Digitalization describes the socioeconomic process and digitization means the technical process [1]. CPS results from the networking of SMAC technologies.

The digitalization of the economy and industry is progressing continuously. One example is the digitalization of the energy sector. The implementation of intelligent electricity meters (so-called smart meters) is creating the necessary communication infrastructure. The most important component is the gateway (Smart Meter Gateway, SMGW), which serves as the central communication unit [2]. Cost and benefit analyses have shown that the construction and operation of this infrastructure are too expensive for the application "smart metering" [3]. For this reason, the infrastructure is being opened up for other divisions and services, such as value-added services. The networking of everyday life in your own home is summarized under the term Smart Home. By networking different sensors and devices, daily life is supported. IoT describes sensors and devices which have a connection to the internet. For example, value-added services can represent the connection of Smart Home or Ambient Assisted Living (AAL) services. Services like Smart Home and AAL are made possible by IoT devices.

By mapping value-added services to the Smart Grid infrastructure, the topics IoT and Smart Grid are linked. This combination creates a highly scalable and volatile system. This leads to a higher volume of data of varying quality, devices and users supplying and accessing data and a high number of participants. One challenge is that the structure of existing architectures is changing and/or expanding. If the existing architectures grow into a highly scalable and volatile system, they must be reconsidered in terms of security.

The existing process models are limited to the analysis of information systems in companies or are models for the development of software under the aspect of security. The consideration and analysis (security modeling and assessment) of highly scalable, volatile systems are not carried out within this frameworks. For future systems, which have the property of being highly scalable and volatile, an appropriate framework for security modeling must be developed. This means, data security according to the requirements of scalability, real-time and a consideration of the overall-process should be represented by the new framework. The aim is the development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems.

The paper is structured as follows. Section II covers the related work. In Section III, we describe the CPS and discuss the topic of security. In the next session, the development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems is performed and Section V, describes the application example. Finally, the conclusion and future work are given.

II. Related work

The state of the art is examined with regard to the following question: Which approaches or frameworks are available for

Copyright (c) IARIA, 2020. ISBN: 978-1-61208-778-8

security modeling of processes in highly scalable, volatile systems or in CPS.

There are best practice approaches for security assessment. These are ISO/IEC 27000:2018 [8] or the BSI-Standards (BSI-Standards 200-1, 200-2 and 200-3 [5]–[7]). Main focus of this security frameworks are the assessment of the business process of a company.

The security modeling is based on a two-level trust model. This means, there are two categories of data: worthy of protection and no worthy of protection [13].

In [9]–[12], security is considered during the development process of software. Another approach are security by design and privacy by design. Security and data protection are already considered during the development process.

Security and privacy considerations for Smart Grid extended by value-added service (e.g., AAL, IoT devices), with a focus on survey and research challenges are shown in [14] and [15]. In [16]–[18], the security and communication analysis of an extended Smart Grid infrastructure are shown.

A survey of literature on security and privacy of CPS is done in [19]. The publication provides an overview of the fields of application and identifies threats and vulnerabilities. In [20], the security analysis is shown on the basis of the different layers (perception layer, transmission layer, application layer).

In summary, these models for security modeling as well as the two-level trust model are not suitable for CPS and high scalable, volatile systems. The models for the security assessment shown, the business process of a company, the software development process and sub-processes of a company are considered. The security and privacy assessment of CPS are open questions.

III. Cyber Physical Systems

CPS are systems in which computing, communication, and control technologies are integrated [21]. There are different types of CPS. In this publication, CPS is described as follows. In CPS, information and software components are combined with mechanical components. The data transfer, data exchange, monitoring and control takes place via the internet and is done in real time. Components are mobile and movable installations, devices and machines, embedded systems and networked objects (IoT). CPS can be described by the following characteristics [22].

- Direct connection between physical world and digital world
- Innovative system functions through information, data and function integration
- Functions integration: multi-functionality
- Soft to hard time requirements
- Extensive interaction networks of sensors or actuators
- Networking within the systems and externally
- Dedicated user interfaces: Strong integration in action sequences
- Use under often difficult physical boundary conditions
- Long-term operation
- Automation, adaptivity and autonomy
- High requirements to:
  - Functional security
  - Access security and data security
  - Reliability
  - High cost pressure

The application field of CPS are production, logistics, mobility, energy and distribution. Smart Grid is a variant of CPSs. The characteristics of future systems are highly scalable, volatile, high data volume and different types of data. For example, the use case ”data logging electricity” shows us that the data flaw from final consumers to the energy supplier. This means for high scalability, two million participants and 192 million consumption values per day. If we have a look inside the communication, there is a data transfer every 15 minutes. This describes the volatility. The next characteristic is high data volume. For example, two million participants generating 22 gigabyte data per day. Different types of data means the diversity of data, like customer data, power consumption or IP address. Further field of application of the Smart Grid infrastructure are Smart Home, gas, water and value-added service.

Security must also be considered by CPS. Until now, the focus has been on robustness and performance. CPSs are fast-growing systems in which personal and sensitive data are also transferred. Furthermore, existing systems and architectures are extended by this. These systems are difficult to define. Security assessment already carried out must be renewed. The requirement criteria for security assessments of CPS are the following.

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

The security assessment of CPS must be developed according to this requirement criteria.

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

In the first step, the requirement criteria data security (DS), scalability (SC) and real-time (RT) are focused. In the context of security modeling of CPS, all three must be considered. The security assessment results from the description of the process by this criteria and is defined as follows: $\text{usecase}_{\text{process}}$ = (DS, SC, RT). The result of the security assessment depends from the description of the process. The framework for the security assessment is as follows. At first, the analysis of the process and infrastructure and also the data and information. The next step is the security assessment against the criteria DS, SC and RT. The last step is the automated mapping

Copyright (c) IARIA, 2020. ISBN: 978-1-61208-778-8

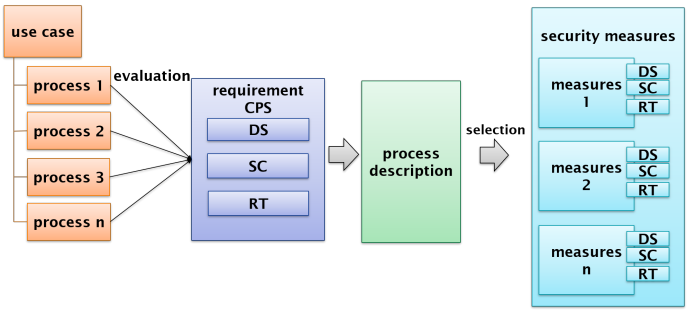

Figure 1. Process-oriented Framework for Security Assessment of Cyber Physical Systems

of the model based on the use case process and assignment of security measures. Further requirements are performance, functional safety, volatility and connectivity. These are not yet considered in the current work status. Figure 1 describes the Process-oriented Framework for Security Assessment of Cyber Physical Systems. The use case is divided into processes. The process is evaluated against the criteria DS, SC and RT. A process description is derived and an automated selection of security measures is possible. The security measures are evaluated by the criteria DS, SC and RT. In the following subsections, the individual characteristics of the tuple are described.

A. Data security

The 4-Level-Trust-Model for safety-critical systems is a model for security assessment of CPS. Classically, the data are divided into two categories - secure and insecure. This describes the classical security model. The 4-Level-Trust-Model for safety-critical systems is one option of the role-based trust model for safety-critical systems [23]. In the new 4-Level-Trust-Model for safety-critical systems the data are categorized in 4 categories. The categorization depends on the requirements analysis for CPS. The 4-Level-Trust-Model for safety-critical systems are defined as follows.

1) Category: non sensitive data
   - All data that do not contain any personal reference or have been made anonymous.
   - There are no effects of damage or damage that has occurred for the affected person.
   - 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 (e.g., network status data).
   - The damage effects are limited and manageable. Any damage that has occurred is relatively easy to heal for the affected person.
   - The security level is minimal.
3) Category: high sensitive data II
   - All data which, through the combination of a further data in categories 2 and 3, have a personal reference, but do not have a direct reference themselves (e.g., status data of a meter).
   - The impact of the damage can be assessed as significant by one person. Damage that has occurred for the person affected can be healed with increased effort.
   - 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 (e.g., name, address).
   - The effects of the damage have reached an existentially threatening, catastrophic extent. Damage that has occurred to the affected person cannot be healed.
   - The security level is high.

The division into four categories is due to the fact that different data are transferred. Data are transferred which are anonymised or does not allow any personal reference (non sensitive data). Furthermore, data are transmitted which are personal data or sensitive data (high sensitive data III). In addition, there is a further database, which is to be classified in two categories (high sensitive data I and high sensitive data II). Table I shows the 4-Level-Trust-Model for safety-critical systems with the coding and the security level. The 4-Level-Trust-Model for safety-critical systems permits to consider the security assessment of data.

TABLE I. EVALUATION CRITERIA DATA SECURITY

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

With the 4-Level-Trust-Model it is possible to evaluate data and information of use case in CPS with regard to security. By subdividing the data worthy of protection, a further gradation between personal data and sensitive data is made. With this model, appropriate security measures can be selected.

B. Scalability

The next criteria is SC. SC describes the number of participants. Participants are understood as users and devices. The scalability is divided in 4 categories (compare Table II).

TABLE II. EVALUATION CRITERIA SCALABILITY

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

The selection of the criteria is based on the Smart Grid use case. "$\leq$ 1" corresponds to one participant and "$2 \leq 100$" corresponds to a networked household. A residential unit is

mapped with the values ”101 $\leq$ 10.000”. The entire network is described with the value from ”$\geq$ 10.001”.

C. Real-time

Another criteria is RT. The RT capability of a system means that a system must react to an event within a given time frame. Table III shows the division into 4 categories.

TABLE III. EVALUATION CRITERIA REAL-TIME

description	coding
$\leq$ 1 sec	0
2 sec $\geq$ 1 min	1
1 min $\geq$ 15 min	2
$\geq$ 15 min	3

The time specifications correspond to the requirements from the Smart Grid use case. Critical values are the requirement for real time ($\leq$ 1 sec) as well as the transmission of measurement data in 15 minute intervals.

D. Summary

With the Process-oriented Framework for Security Assessment of Cyber Physical Systems it is possible to evaluate the process of use case in CPS regard to DS, SK and RT. With the achievement of this result, the appropriate security measures can be selected.

V. USE CASE EXAMPLE

Secure Gateway for Ambient Assisted Living (SEGAL) is a publicly funded research project and describes a value-added service. The aim of the project is the development of the SEGAL service, based on the use of AAL devices (IoT devices) and the Smart Grid infrastructure. AAL data collected within an AAL environment are recorded manually and automatically by sensors and forwarded to an external control center for processing. The AAL environment consists of digital assistants (Alexa or Google Home Mini, etc.), AAL-Devices (sphygmomanometer, heart rate monitor, etc.) or Smart Home devices (smoke detector, thermostat etc.). The communication takes place via a SMGW. The SMGW is connected to the AAL-Hub. The AAL-Hub connects the sensors, managed the communication with the gateway and the resulting data are aggregated.

A. Analysis of the application

The first step is the analysis of process, infrastructure, data and information. The use case SEGAL is divided into the following process:

- Process 1: Initialize device
- Process 2: Delete device
- Process 3: Update
- Process 4: Transmit data
- Process 5: Transmit emergency data

In the context of further analysis, we regard to the processes ”process 1: initialize device” and ”process 5: transmit emergency data”. In case of ”process 1: initialize device”, the following data are transmitted (compare Figure 2).

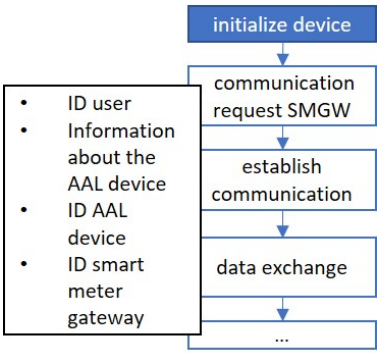

Figure 2. Process 1: Initialize device

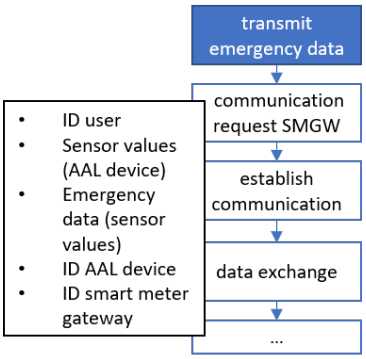

Figure 3. Process 5: Transmit emergency data

- ID user
- Information about the AAL device
- ID AAL device
- ID SMGW

In case of ”process 5: transmit emergency data”, the following data are transmitted (compare Figure 3).

- ID user
- Sensor values (AAL device)
- Emergency data (sensor values)
- ID AAL device
- ID SMGW

B. Security assessment

The next step is the security assessment. The security assessment is divided in DS, SK and RT.

1) Data security: The data security assessment for process 1: initialize device is the third category ”high sensitive data” (compare Table IV). ID user, information about the AAL device, ID AAL device and ID SMGW are no personal data, but data which have in combination of a further data in categories 2 and 3, have a personal reference, but do not have a direct reference themselves.

The data security assessment for process 5: transmit emergency data is the third category ”high sensitive data” (compare

Copyright (c) IARIA, 2020. ISBN: 978-1-61208-778-8

Table IV). ID user, sensor values, emergency data, ID AAL device and ID SMGW are no personal data, but data which have in combination of a further data in categories 2 and 3, have a personal reference, but do not have a direct reference themselves.

TABLE IV. OVERVIEW: DATA SECURITY

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

2) Scalability: If we consider the scalability in process 1: initialize device, we find out that we have between 2 and 100 participants (compare Table V). The coding of the criteria scalability for the process 1: initialize device is "1".

The scalability of process 5: transmit emergency data is "1" (compare Table V). There are participants between 2 and 100 participants.

TABLE V. OVERVIEW: SCALABILITY

process	description	coding
1	$2 \leq 100$	1
5	$2 \leq 100$	1

3) Real-time: The requirement real-time of "process 1: initialize device" is not given and the coding is "2" (compare Table VI).

In case of "process 5: transmit emergency data" the requirement real-time is given (compare Table VI). The coding of process 5 is "0".

TABLE VI. OVERVIEW: REAL-TIME

process	description	coding
1	1 min $\geq$ 15 min	2
5	$\leq$ 1 sec	0

4) Summary: The result of the assessment is the following description of the respective processes.

- $\text{SEGAL}_{\text{process1}}$ = (2,1,2)
- $\text{SEGAL}_{\text{process5}}$ = (2,1,0)

The evaluation provides a statement about how security critical the process is and a statement about SC and RT requirements. The example of the use case SEGAL illustrates that the difference can be seen in the RT requirement, while maintaining the same level of DS and SC. This must be taken into account when selecting suitable security measures.

C. Automated mapping of security measures

The last step is the automated assignment of the appropriate security measures. The security measures are also evaluated according to the CPS requirement criteria. The evaluation of security measures using the example of authentication is work in progress.

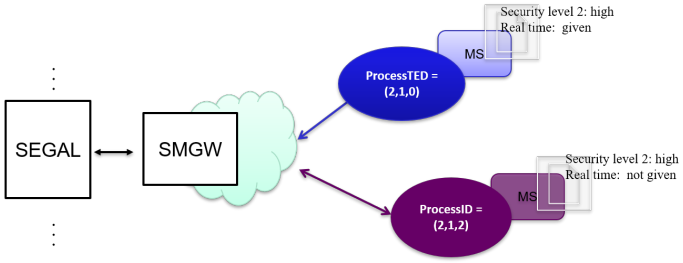

Figure 4. Use case SEGAL

D. Summary

With this example, it can be shown that the evaluation of DS and SC is the same. The difference between the use cases is the RT requirement. With the result obtained, appropriate security measures can be selected for the use case. Security measures, such as authentication, must be selected based on the real-time requirement criterion (compare Figure 4).

VI. Conclusion and Future Work

In this paper, we presented the problem of security in future highly scalable and volatile systems. Based on the requirement criteria we developed the Process-oriented Framework for Security Assessment of Cyber Physical Systems. The model consists of the following steps: analysis of the application, security assessment, automated mapping of security measures. We showed the application of the model using the SEGAL use case. The use case showed us the necessity, different evaluation of security in CPS.

The Process-oriented Framework for Security Assessment of Cyber Physical Systems is a new framework for security assessment of CPS. With this model it is possible to evaluate use cases and processes in highly scalable, volatile systems and to select security measures such as authentication in a targeted manner. The model is intended to provide practical assistance in the evaluation of processes and use cases in highly scalable, volatile systems. The next steps are the automation of the framework, the definition of the security measures and the extension of the framework with the criterion performance, functional safety and volatility.

References

[1] C., Legner, et al., Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community, Bus Inf Syst Eng 59, pp. 301–308, 2017.

[2] M. Irlbeck, Digitalisierung und Energie 4.0 – Wie schaffen wir die digitale Energiewende?, Springer Fachmedien Wiesbaden GmbH, pp. 135-148, 2017.

[3] Ernst u. Young GmbH, Kosten-Nutzen-Analyse fuer einen flaechendeckenden Einsatz intelligenter Zaehler, 2013.

[4] ISO/IEC Information Technology Task Force, ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018.

[5] Federal Office for Information Security (Germany), BSI-Standard 100-1 Managementsysteme fuer Informationssicherheit (ISMS), 2008, [Online]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile&v=2 [retrieved: 08, 2020].

Copyright (c) IARIA, 2020. ISBN: 978-1-61208-778-8

[6] Federal Office for Information Security (Germany), BSI-Standard 200-2 IT-Grundschutz Methodology, 2017. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=1 [retrieved: 08, 2020].

[7] Federal Office for Information Security (Germany), BSI Standard 200-3: Risk Analysis based on IT Grundschutz, 2017. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2 [retrieved: 08, 2020].

[8] ISO/IEC Information Technology Task Force, ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018.

[9] R. Matulevičius, et al., Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development, International Conference on Advanced Information Systems Engineering, pp. 541-555, 2008.

[10] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos, Tropos: An Agent-Oriented Software Development Methodology, Autonomous Agents and Multi-Agent Systems 8, pp. 203–236, 2004.

[11] D. Mellado, C. Blanco, and L. Sanchez, A systematic review of security requirements engineering, Computer and Standards & Interfaces, Volume 32, Issue 4, pp. 153 – 165, 2010.

[12] L. Compagna, P. El Khoury, A. Krausová, F. Massacci, and N. Zannone, How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns, Artif Intell Law 17, pp. 1–30, 2008.

[13] K. Boroojeni, M. Amini, and S. Iyengar, Smart Grids: Security and Privacy Issues, Springer International Publishing, 2017.

[14] F. Dalipi and S. Y. Yayilgan, Security and Privacy Considerations for IoT Application on Smart Grids. Survey and Research Challenges, IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 63-68, 2016.

[15] M. Yun and B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, International Conference on Advances in Energy Engineering, pp. 69-72, 2010.

[16] B. Genge, A. Beres, and P. Haller, A survey on cloud-based software platforms to implement secure smart grids, 49th International Universities Power Engineering Conference (UPEC),pp. 1-6, 2014.

[17] S. Bera, S. Misra, and J. Rodrigues, J.P.C: Cloud Computing Applications for Smart Grid. A Survey, IEEE Trans. Parallel Distrib. Syst. 26 (5), pp. 1477-1494, 2015.

[18] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds, IEEE 4th USENIX International Conference on Cloud Computing (CLOUD), pp. 582-589, 2011.

[19] A. Humayed, J. Lin, F. Li, and B. Luo, Cyber-Physical Systems Security—A Survey, IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802-1831, 2017.

[20] Y. Ashibani and Q. H. Mahmoud, Cyber physical systems security: Analysis, challenges and solutions, Computers & Security, Volume 68, Pages 81-97, 2017.

[21] K. Kim and P. R. Kumar, Cyber–Physical Systems: A Perspective at the Centennial, Proceedings of the IEEE, vol. 100, no. Special Centennial Issue, pp. 1287-1308, 2012.

[22] M. Broy, Cyber-Physical Systems — Wissenschaftliche Herausforderungen Bei Der Entwicklung, Cyber-Physical Systems acatech DISKUTIERT, pp. 17-32, 2010.

[23] K. Neubauer, S. Fischer, and R. Hackenberg, Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT, ARCS Workshop, 32nd International Conference on Architecture of Computing Systems, pp. 1-6, 2019.

Copyright (c) IARIA, 2020. ISBN: 978-1-61208-778-8