A Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
"Doctor rerum naturalium" der Georg-August-Universität Göttingen

im Promotionsprogramm Computer Science (PCS)
der Georg-August University School of Science (GAUSS)

vorgelegt von
Katrin Neubauer

aus Freyung
Göttingen, 2022

Betreuungsausschuss

Prof. Dr. Ramin Yahyapour
Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen mbH (GWDG),
Institut für Informatik, Georg-August-Universität Göttingen
Prof. Dr. Rudolf Hackenberg
Fakultät für Informatik und Mathematik, Ostbayerische Technische Hochschule Regensburg

Mitglieder der Prüfungskommission:

Referent: Prof. Dr. Ramin Yahyapour
Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen mbH (GWDG),
Institut für Informatik, Georg-August-Universität Göttingen
Koreferent: Prof. Dr. Rudolf Hackenberg
Fakultät für Informatik und Mathematik, Ostbayerische Technische Hochschule Regensburg

Weitere Mitglieder der Prüfungskommission:

Prof. Dr. Andreas Aßmuth
Fakultät Elektrotechnik, Medien und Informatik, Ostbayerische Technische Hochschule Amberg-Weiden
Prof. Dr. Marcus Baum
Institut für Informatik, Georg-August-Universität Göttingen
Prof. Dr. Jens Grabowski
Institut für Informatik, Georg-August-Universität Göttingen
Prof. Dr. Dieter Hogrefe
Institut für Informatik, Georg-August-Universität Göttingen

Tag der mündlichen Prüfung: 12.07.2022

Acknowledgements

It is time to say thank you to all those outstanding people who have guided me during my work on this dissertation.

First, I would like to thank my thesis advisor, Prof. Dr. Ramin Yahyapour, for his guidance, continuous support and fruitful discussions throughout. I would also like to thank my second supervisor, Prof. Dr. Rudolf Hackenberg, for the numerous and tireless academic conversations, inspiring discussions and for the continuous support during the time of research, study and writing of this thesis. The encouragement and support of Prof. Dr. Rudolf Hackenberg has made this work possible. Thank you for the opportunity to present at research conferences and for the freedom and time to explore my research interests.

A special thanks goes to the project consortium of Smart Energy Management Program (SEMP) and Secure Gateway Service for Ambient Assisted (SEGAL) Living especially Gordon Speda and Alois Schmid, who gave me access to the industrial side of the research. Also, the many non-scientific and motivating talks have supported my work.

I would like to thank my colleagues at the Laboratory for Information Security and Compliance of the Ostbayerische Technische Hochschule Regensburg for the many discussions, support and generation of new research ideas.

I would also like to thank the Landeskonferenz der Frauenbeauftragten an Bayerischen Hochschulen for the PhD scholarship and the opportunity to network and exchange ideas with other female researchers.

Last but not least, I would like to thank my family and closest friends. They have been with me through all my ups and downs during the course of my work and have always supported me. Thank you mom and dad.

Abstract

Due to digitalization and technological advancement, systems and their requirements are changing, and there is an increasing use of Cyber-Physical Systems (CPS) with a direct connection between the physical and the digital world. These systems process data and have integrated functions and a real-time requirement. There is a great need for security, protection of data, and reliability. The use of digital systems in the energy sector is increasing and changing, as are consumers and generators. This requires a secure IT, communications infrastructure, and highly performing data platforms. The new systems being created are called CPS, which are highly scalable, dynamic, and volatile and process many data of various kinds.

One significant aspect of a CPS is security. Personal data and business-sensitive data may be processed, or mission-critical processes may be mapped. Risk analysis and security assessments based on conventional methods and guidelines (for example, BSI IT Basic Protection) have revealed drawbacks. Present security assessment methods focus on analyzing corporate information systems or are applied for software development life cycles. CPS criteria and their impact on security have not yet been accounted for in today's security assessments and their corresponding frameworks.

This thesis concentrates on modeling CPS security and deriving a framework for CPS security assessments. The considered criteria are data security as conventional, expanded by scalability, and real-time. The underlying framework is process-oriented. CPS use cases will be broken down into (atomic) processes and the security assessed based on each process' data security, scalability and real-time model. Eventually, this will mean security measures can be mapped at the process level. Conducting this research, the focus was on smart grid systems as one example of CPS. For the discussion of mapping security measures, authentication was selected.

The result analysis shows an added value in the security assessment of CPS based on the criteria of data security, scalability, real-time, and the breakdown at the process level. The underlying model allows to cope with the complexity of CPS and more precisely assess the security of CPS. The overall approach of CPS security modeling and provision by using a process-oriented framework is highly innovative and provides a concept for developing future CPS security assessment tools.

Contents

List of Figures

List of Tables

List of Abbreviations

AAL	Ambient Assisted Living
AOP	Agent Oriented Programming
BDEW	Bundesverband der Energie- und Wasserwirtschaft e.V.
BDSG	German Federal Data Protection Act
BSI	German Federal Office for Information Security
CA	Certification Authority
CPS	Cyber Physical Systems
DS	Data Security
Drops	Dimensionally Relational Organization and Problem-based Security Model
EEG	Renewable Energy Act
EnWG	Energy Industry Act
EVU	Energy Supplier
GDPR	European General Data Protection Regulation
HAN	Home Area Network
iMSys	intelligent Measuring System
IoT	Internet of Things
ISO	International Organization for Standardization
LMN	Local Metrological Network
MsbG	Metering Point Operation Act
mME	modern Measuring System
PKI	Public Key Infrastructure
PROSA	Process-oriented Framework for Security Assessment of Cyber-Physical Systems
RA	Registration Authority
RE	Renewable Energy
RFID	Radio Frequency Identification
RT	Real-time
SC	Scalability
SEGAL	Secure Gateway Service for Ambient Assisted Living
SEMP	Smart Energy Management Program
SMGW	Smart Meter Gateway
SMGWA	Smart Meter Gateway Administrator
VDE	German Association for Electrical, Electronic & Information Technologies
WAN	Wide Area Network

Chapter 1

Introduction

Nowadays, it is hard to imagine life without Cyber-Physical Systems (CPS). The number of networked devices has been growing steadily in recent years with no foreseeable changes in the near future. Whether in everyday life or road traffic, CPS are everywhere and support people with, for example, location-based weather forecasts or with reversing sensors in cars. Despite the many advantages, the security of the systems must not be disregarded. This raises the question of whether today's security assessment methods can still cope with the ever higher scaling of systems and guarantee the necessary level of security. In the following, the topic of this thesis is introduced, and the research objectives are presented.

1.1 Overview

Digital transformation has found its way into business and private life. It consists of digitization and digitalization. While digitization concerns technical processes, digitalization involves socio-technological change. With the increasing digitalization in our world, new technologies, like the Internet of Things (IoT), will greatly influence our future way of life [1]. However, not only are private technologies increasing their digitalization, but the future smart grid is also a highly networked system. In order to use these innovative services, which have emerged from digitalization, volatile and highly networked systems are necessary. Volatile and highly networked systems are described as CPS. The increasing establishment of CPS creates new challenges for security and data protection.

In Germany, integrating the intelligent energy supply system (smart grid) creates a new IT infrastructure. The intelligent measuring system (iMSys), containing a basic meter (smart meter) and the smart meter gateway (SMGW) [2], is currently being installed in many households and companies in Germany. The digitalization of the electricity grid, however, brings new dangers and challenges in security and data protection. In a worst-case scenario, this can lead to cyber-attacks without the necessity of physical access to the network. Besides the smart grid, all kinds of devices can connect to the internet. These devices can range from smart refrigerators to connected cars and are called IoT. Most of the time, existing devices have a communication interface and are either directly connected to the internet or managed via a gateway.

CPS, just like the smart grid, also brings new security and safety dangers. For consumer devices, usually, there is no excessive damage. Yet, the lack of security in consumer devices connected to other networks can lead to serious damage in other (critical) infrastructures. One big challenge is the high number of newly connected devices. Services for only a few devices are getting new ones on a large scale which are not necessarily persistent. They are flexible and appear as well as disappear quickly during their lifetime. This volatility is a big challenge for the security of existing and new services [1]. Through new technologies, existing systems evolve and become complex systems. In these systems, the characteristics of CPS can be considered. The smart grid can be mentioned here as an example. In addition to the classic use cases, so-called value-added services will also be mapped in the future. This leads to new challenges in terms of security assessment, both in the smart grid example and in general. These new types of systems must be evaluated in terms of security in order to be able to implement suitable security measures.

New volatile and highly scalable systems (CPS) are emerging, which bring new challenges in terms of security and data protection. CPS are required for existing and future applications to offer new services (for example, value-added services or energy regulation in the grid). In this context, CPS data security and security assessment must be analyzed.

1.2 Research Context

CPS are the next generation of engineered systems. CPS are a new generation of systems with integrated computational and physical capabilities. For technological progress, the ability to interact with the physical world and extend capabilities through computation, communication and control is a significant factor [3]. The digitalization of the economy and industry is progressing continuously, for instance, by the digitalization of the energy sector. The future smart grid can be described as a complex system-of-a-system. The need to use information and communication technology between the various components involved in the processes is an aspect that is becoming increasingly important. An overriding goal to be achieved by smart grids relates to aspects such as the optimization and coordination of the various elements and their operation in the transmission and distribution network [4]. The implementation of intelligent electricity meters (so-called smart meters) creates the communication infrastructure needed. The most important component is the gateway (Smart Meter Gateway, SMGW), the central communication unit [2]. Cost and benefit analyses have shown that the construction and operation of this infrastructure are too costly for the application of “smart metering” [5], so the infrastructure is being opened up for other divisions and services, such as value-added services. The networking of everyday life at home has been given the label *smart home*.

By networking different sensors and devices, daily life is supported. The IoT is a sobriquet describing sensors and devices that connect to the internet. A further example of a value-added service is Ambient Assisted Living (AAL). Services like smart home and AAL are made possible through IoT devices.

Value-added mapping services link IoT and the smart grid to a smart grid's infrastructure. The smart grid infrastructure is used for other use cases in addition to the classic use cases of the energy industry, such as smart metering. These are, for example, value-added services with the integration of a smart home. Other areas of application can be found in other sectors, such as reading the current water consumption. Mapping the use cases in the smart grid infrastructure creates a highly scalable and volatile system, leading to a higher volume of data of varying quality, a higher number of devices and human users supplying and accessing data, and an increased number of participants. One challenge is that the structure of existing architectures is changing and/or expanding, as they grow into a highly scalable and volatile systems and, therefore, must be reviewed in terms of security. The question arises as to how these newly developing systems can be evaluated with regard to data security. Are the existing procedures for secuirty assessment still suitable for these systems in practice, or do they need to be adapted?

The existing process models for security assessment are limited to companies' analysis of information systems, or are models for software development under security. Research (security modeling and assessment) into highly scalable, volatile systems is not being carried out within these frameworks. In classical security assessment, the focus is on security. The question arises whether the sole security consideration in CPS is still sufficient. In the classic approach, security is assessed by dividing it into three categories (low, medium, and high). If we look at the smart grid application example here, the 3rd category "high" includes many data and information. All data, not just personal data, is assigned to the third category [6]. This means that all processes and systems must implement the highest security measures. A system with a vast number of participants, a very high volume of communications, and a high volume of data can quickly reach its limits under these conditions. Hence, it is necessary to develop a new evaluation scheme and adapt the trust modeling to meet the requirements.

Due to the system structures and the characteristics of CPS, it is no longer sufficient to consider only the criterion of data security. Additional criteria for security assessment must be defined. Another aspect due to the characteristics of CPS is that the processes must be considered as a whole. This is especially true when data is collected using different systems and locations. In addition to security assessment, a further issue is the selection of security measures, which must be reconsidered with the aspect of CPS. The question arises as to whether every security measure is suitable for CPS and whether these must also be analyzed with regard to the requirements of CPS. For future systems, which will be highly scalable and volatile, an apt framework for security modeling must be developed to meet the needs for scalability, real-time, and a consideration of the process as a whole. In addition to these significant features the framework must also map the process of selecting appropriate security measures. The aim is to establish a Process-oriented Framework for Security Assessment of Cyber-Physical Systems (PROSA). In the following, the framework will be referred to as PROSA.

This aim leads to the question underlying the present research: *How does security for highly scalable, volatile systems work in the application of the smart grid? The valid trust model must be developed further to consider the requirement of security in highly scalable and volatile systems and to master the future flow of data flow and thus reduce the grid's complexity.*

This work strives to develop a process-oriented framework model for automated security assessment in CPS. CPS are novel, complex systems with new requirements in terms of security assessment. Among other things, CPS are highly scalable and volatile, involving real-time processing with high security requirements. This leads to new challenges in security assessment as well as in the included trust modeling and selection of appropriate security measures. The security assessment and trust modeling are generated based on the requirements of CPS. The criteria for the security assessment in CPS have to be defined. Furthermore, the framework should enable an automated selection of security measures. The contribution of this thesis is the development of a process model, which has been adapted for the security assessment of CPS. A process-oriented framework has been developed, which represents the entire process of security assessment. Application areas are described in atomic processes and evaluated according to the criteria of data security, scalability and real-time. With the result of the security assessment, the corresponding security measures, which were also previously assessed on the basis of these three criteria, can be automatically assigned. In this work, the security measure "authentication" was selected as an example. The criterion of data security will be further defined in the context of the model development and a new trust modeling will be introduced. The model will be verified in practice by means of an empirical study in the smart grid use case. It shows that the process-oriented framework in the smart grid use case provides added value through the other use cases for security assessment. In addition to the study, this is also shown by a proof of concept. Here, a process-oriented authentication concept was developed, which was tested on the basis of the use case. The process-oriented framework can be automated. This means that both the security assessment as well as the selection of security measures can be automated. This is the prerequisite for the framework to be used as a software-based security assessment. Here the possibility exists to develop a new software tool or to adapt existing ones. The process-oriented framework was developed and tested on the basis of the smart grid application area. The approach can be abstracted and adapted for any application area of CPS. The criterion of data security is universal. The criteria of scalability and real-time requirement must be adapted to the respective application areas. The applicability in further sectors is shown using the example of autonomous mobility.

The contribution of this work is, in general, the consideration of security assessment in the context of CPS. The goal is to develop a process model for the evaluation of security in CPS that is process-oriented, automatable, and tool-supported, and that can be used to make an automatable selection of suitable security measures. This thesis outlines a new framework, and the question posed.

1.3 Structure of the Thesis

The thesis is structured as follows. Chapter 2 covers the background of the research context. Chapter 3 presents an overview and the structure and application of CPS. Chapter 4 introduces a smart grid. Chapter 5 is concerned with stating the problem. Chapter 6 outlines the related work and requirements analysis. Chapter 7 covers the model development of PROSA and the case study. Chapter 8 presents the proof of concept. The results of the analysis are shown in Chapter 9. Chapter 10 covers the extent to which PROSA can be applied to other systems and is followed by the conclusion and possibilities for future work.

This scientific work is based on the publications I have published in this research context (see Appendix B). The requirements analysis, which includes the state of the art in science and technology, and the model development have been published in [7], [8], [9] and [1]. In [7] and [8], the model for the evaluation criterion of data security (4-Level-Trust-Model) is presented in addition to the state of the art and the presentation of the union of the smart grid and IoT architectures. The 4-Level-Trust-Model is presented in [1] in the context of a security analysis of IoT. The PROSA security assessment approach is presented in [9].

Chapter 2

Background

In today's world, the topic of CPS is ubiquitous. The interconnection of mechanical components via networks with the help of modern information technologies is used in almost all industries. One of these is the energy industry, in which a new information and communication infrastructure (smart grid) is being established. The higher the degree of networking, the more information is sent via the interconnected networks and communication channels, and the more complex the system. Despite the new possibilities, the security factor must not be lost sight of. The system's security is crucial, especially in essential systems, such as an intelligent power grid (smart grid). This chapter covers the basic concepts in this field of research and introduces the terms security and privacy, security assessment, CPS, and smart grid. They are then used as defined.

2.1 Overview

"Blackout" [10] is a science fiction book by Marc Elsberg about a fictional collapse of the European power grid. In "Blackout", the power cut is triggered by a hacker attack and lasts for a total of almost two weeks. Fiction or reality? Considering the continuous digitalization of today's world, the danger of this fictional scenario doesn't seem completely absurd.

The power grid consists of a large number of networks whose components are monitored and controlled by computers or programmable logic controllers. This presents a potential target for hackers. A power grid consists of thousands of units linked to each other via data and control lines, which work in precise coordination with each other. If one component fails, it generally only affects part of the grid. A targeted cyber attack on neuralgic nodes, on the other hand, could affect an entire country [11]. In addition to security of supply, an important aspect is data security. Attackers can target not only supply security, but also the data and information that is collected as part of the energy industry's business processes. In addition to sensitive company data, this can also include customer data and information about the network.

The power grid described above can be classified as a CPS. CPS are systems with interactions between the digital and physical worlds. They are systems in which information and software technology are connected with mechanical components. Data transfer and exchange, as well as control and regulation, take place in real-time via a network such as the Internet.

The book “Blackout” is currently fiction. However, the danger of an attack on the power grid has been steadily increasing in recent years. Due to the technological development of the power grid from a simple grid to a very complex grid, the danger of attacks is also increasing. The power grid has evolved over the last decade into a CPS with new requirements for security in general and data security in particular.

2.2 Security and Privacy

The effects of ongoing digitization are having a major impact on our private daily lives as well as on corporate processes and business models. Due to the constantly increasing amounts of data that are collected, stored and processed, individuals and companies are becoming more and more vulnerable to data theft and misuse [12]. When companies are blackmailed with data loss, it can be concluded that there is a lack of security. As a rule, not only individual processes are at risk, but the company as a whole [13]. Security and privacy are factors that must be considered in every phase of a company’s development in general, and its processes and applications in particular.

Security and privacy are crucial in every field of application. A distinction can be made between safety (also known as fail-safety) and security of data (also known as data security or information security). In this thesis, we shall be focusing on “data security”. Due to an increasing amount of processing, data protection is becoming more important.

2.2.1 Data Security

Security of information is a property of a functionally secure system, namely to assume only such states that do not modify or acquire unauthorized information [14]. The main aims of information security are defined as follows:

Integrity: Information is only accessible to authorized persons. No unauthorized information can be obtained.

Confidentiality: Information is only modified by authorized persons in an intended manner. This means no unauthorized modification of information.

Availability: Information is available at all times or within a specified period of time.

This thesis is about information security, referred to below as data security.

2.2.2 Privacy

Privacy in the narrow sense of the word, as defined, among other things, by the German Federal Data Protection Act (BDSG) or by the current European General Data Protection Regulation (GDPR), is taken to mean the ability of natural people to control the disclosure of information about them. This includes, in particular, security requirements set by German legislators to guarantee the right to informational self-determination [14]. The principles of data protection apply to the permission to use data, the right to withhold data, the economic use of data, earmarking, transparency and the use of direct surveys [15].

- Permission reservation: data processing is permitted only with given consent.
- Data avoidance: the processing of personal data must be appropriate and relevant to the aim and be needed for the processing.
- Data economy: data should neither be stored indefinitely nor deleted when not required.
- Earmarking: personal data should be collected and processed for only explicit aims.
- Transparency: persons affected should know for how long data and information about their transfer are stored.
- Direct survey: data should be collected directly from a person affected.
- Necessity: data may be stored if this serves the aim.

Privacy is not explicitly considered in the context of this thesis. Security assessment also implies privacy.

2.3 Security Assessment

In an age where new threats and vulnerabilities are discovered almost daily, it is of great importance to assess systems in terms of security. Through security assessment, companies can correctly evaluate the security of their systems as well as threats and vulnerabilities [16].

The security assessment methods comprise a methodology to assess systems with regard to security. It aims to evaluate systems or processes in terms of security and can make a statement about the level of security. The assessment also has the goal of verifying compliance with rules. The security assessment of systems can also identify vulnerabilities. This security assessment has the special feature that a recurring process is established for the assessment of systems [17].

The methods for security assessment can be used to evaluate systems with regard to data security. The security assessment is based on the basic objectives of data security. With the successful establishment of a security assessment process, the security of systems can be increased.

2.4 Cyber-Physical Systems

Information and communication technologies are strong drivers of innovation. The two main drivers are embedded software-intensive systems and global networks such as the Internet and the data and services available on the World Wide Web. These two strong fields of innovation are converging to form CPS [18].

There are different definitions of CPS. In this context, CPS is interpreted and defined as voiced by Helen Gill at the National Science Foundation in the US in 2006 [19]:

> *"Cyber-physical systems are physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is ›deeply embedded‹ into every physical component, possibly even into materials. The computational core is an embedded system, usually demands real-time response, and is most often distributed."*

CPS combines tightly integrated physical processes, networks, and computation. The physical process is monitored and controlled by embedded (cyber) subsystems via networked systems with feedback loops to change their behavior. These subsystems operate independently and can interact with the external environment. Multiple tiny devices implement the physical processes with sensing, computing, and communication capabilities (often wireless). These physical devices can be identified by physical attributes or information-capture devices such as infrared sensors or radio frequency identification (RFID). They can also be connected to a network system, in most cases the Internet, to send the captured data to the computational subsystem [20].

A CPS can be taken to be a system whose visible boundaries are fuzzy. The subsystems involved are complex, and the data vary in their quality, origin, and sites.

2.5 Smart Grid

The socio-politically desired transformation of the energy supply system in Germany, which in the future will be based almost entirely on renewable energies and thus predominantly fluctuating generation, is in full swing [21]. Over the next few decades, an energy supply system based predominantly on fossil fuels (currently almost 80 %) is to be converted to a high proportion of renewable energies [22]. At the same time, the declared goal at the European level is to create a single internal electricity market. These trends in the national and European energy transition are irreversible and pose new and major challenges for the transmission system operator in its core tasks of building and operating grids, providing market and grid access, and integrating renewable energies.

One challenge that can be mentioned here is digitization. It describes the real-time or online or short-cycle ex-post availability and intelligent processing of large amounts of data, which allows relevant information to be made available for efficient system control. With appropriate digitization to ensure sufficient observability and controllability of system components, supraregional and regional grids are referred to as “smart grids” [21].

The European Commission has defined the term “smart grid” as follows:

“A Smart Grid is an electricity network that can cost efficiently integrate the behavior and actions of all users connected to it – generators, consumers and those that do both – to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.” [23].

The German Association for Electrical, Electronic & Information Technologies (VDE) has made this definition more specific and interpreted it for the German market. The VDE defines a smart grid as follows: A smart grid (intelligent energy supply system) comprises the networking and control of intelligent generators, storage units, consumers, and network operating equipment in energy transmission and distribution networks with information and communication technology [24]. This definition is used in the context of this thesis.

A smart grid has a decentralized structure. Consumption data is recorded and billed decentrally, and the system is controlled, operated, and maintained decentrally. It consists of a variety of heterogeneous systems and is complexly networked. Controlling and embedded systems such as sensors, actuators and physical and operational processes are integrated and connected via various networking technologies, including the Internet, to form an overarching, networked system. Such systems combine autonomous, low-resource physical devices such as smart meters with high-resource backend and information management systems [25].

2.6 Summary

In this chapter, the key areas of security, security assessment, CPS and smart grid have been defined. In summary, it can be said that the significance and importance of security is increasing. The focus of this work is on data security with its basic objectives of availability, confidentiality and integrity. As the importance of CPS is steadily increasing, these systems are to be understood as the technological advancement of existing systems. CPS are systems where the visible boundaries of a system become blurred. The subsystems involved are complex as well as highly interconnected. As there are several different types of participants in a CPS, the produced data varies in quality, origin and occurrence. Smart grid is an application example of CPS. It describes the digital transformation of the energy grid towards an intelligent energy supply system. In CPS and the application of smart grid personal data or data requiring special protection are transmitted, processed and stored. In general, the evident question of security is deeply connected to the specific need for data security. But how can data security be ensured in future systems (CPS)? And how can these procedures be mapped with the existing frameworks for security assessment? In the following chapter, CPS are presented in more detail and the challenges and requirements for security assessments are elaborated.

Chapter 3

Cyber-Physical Systems

The term “Cyber-Physical Systems” is extensive and encompasses a wide range of different systems and applications. Nevertheless, CPS have specific properties and characteristics that are widely accepted and considered typical. Therefore, there are many different manifestations of such systems, and they can thus be used in many different application scenarios. This chapter presents the topic CPS. After a brief overview of CPS, the structure and field of application will follow as well as security assessment for CPS.

3.1 Overview

The embedded system plays an important role and is usually part of CPS. An embedded system differs fundamentally from a classic computing system. The classical computing system (computer or PC) performs various and ever-changing tasks with the help of software systems and has not been designed for a specific application. In contrast, embedded systems are only used in exceptional environments and are optimized precisely for this purpose. Thus, specialized hardware works together with the corresponding software to execute the respective application efficiently. Another vital component of CPS is the Internet or, to put it another way, the possibility of networking systems worldwide. Thus, networked embedded systems result in the so-called CPS [19].

CPS integrate computation with physical processes. Embedded computers and networks monitor and control physical processes, usually with feedback loops in which physical processes affect computations and vice versa. In the physical world, time inevitably passes, and simultaneous events are inseparable. Neither is true in today’s abstractions of computers and networks [26]. Data transfer and exchange, and monitoring or control, occur in real-time over a network such as the Internet. The components may consist of mobile and movable equipment, devices and machines (including robots), embedded systems, and networked objects. The challenges for CPS consist of the standardization and integration of components, system verification, complexity reduction, increased security and data protection, and the assessment of these. The following features are typical of CPS (compare Figure 3.1) [27].

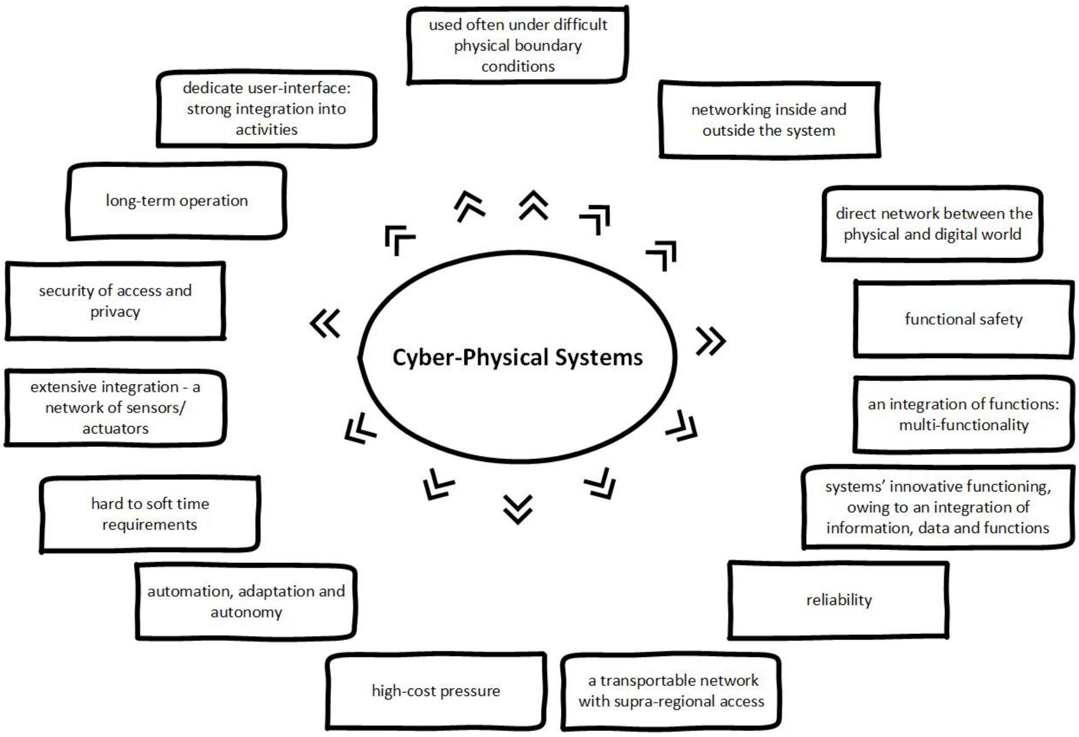
used often under difficult physical boundary conditions
dedicate user-interface: strong integration into activities
networking inside and outside the system
long-term operation
direct network between the physical and digital world
security of access and privacy
functional safety
Cyber-Physical Systems
extensive integration - a network of sensors/ actuators
an integration of functions: multi-functionality
hard to soft time requirements
systems' innovative functioning, owing to an integration of information, data and functions
automation, adaptation and autonomy
reliability
high-cost pressure
a transportable network with supra-regional access

FIGURE 3.1: Features of Cyber-Physical Systems

CPS directly connect the physical and digital world. This means that in CPS, sensors and actuators communicate directly with real system, such as production systems. In the example of the smart grid, the communication of smart meters, communication units, smart home devices, energy providers, or even customers can be considered. These new possibilities also result in new types of system functions. This is accredited by integrating information, data and tasks in CPS. By networking different sensors and actuators, new data and information pools are created that enable new services. CPS can be described as a multi-functional network with supra-regional access. Requirements for time can be considered in CPS, which are described as hard and soft in literature. CPS find applications in critical infrastructures with hard time requirements (for example, the energy industry). The described characteristics lead to extensive interaction. In CPS, large networks with sensors and actuators are created, which lead to extensive interaction. Networking in CPS can be observed on the one hand within the systems and on the other hand externally. CPS lead to a strong integration in action sequences and can thus be described as dedicated user interfaces. Application often takes place under difficult physical boundary conditions. CPS are designed for long-term operation by building complex system structures. CPS are suitable for automating processes. In general, CPS pose a challenge for functional safety, security of access and privacy, reliability, and high-cost pressure. It is necessary to ensure the fail-safety of the systems and their reliability. CPS are used in sensitive areas as well as in critical infrastructures. Due to the processing of personal and company-relevant data, access security and data protection must also be guaranteed. Compliance with the requirements described here leads to immense operating costs. Companies are increasingly encouraged to save on operating costs, which is a requirement for developing and using such systems.

3.2 Applications and Structure of Cyber-Physical Systems

CPS unify the emerging application of embedded computing and communications technologies in various physical domains. The CPS phenomenon can be observed in aerospace, automotive, chemical manufacturing, civil infrastructure, energy, healthcare, manufacturing, materials, transportation, etc [28]. There are a number of use cases for CPS (see Figure 3.2), both in the private sector and in industry. With the help of the electronic networking of sensors and actuators in modern household appliances, the so-called IoT can be implemented. In the industrial sector, the buzzword Industry 4.0 is very present. This involves more efficient and cost-effective production through self-controlling production systems. Another use case is the transportation industry. Rail and air traffic benefit significantly from the reliable operation of highly networked systems. It is also used in the automotive industry: With the help of a wide variety of sensors and actuators, drivers are offered assistance that would not be possible without high-level networking [19].

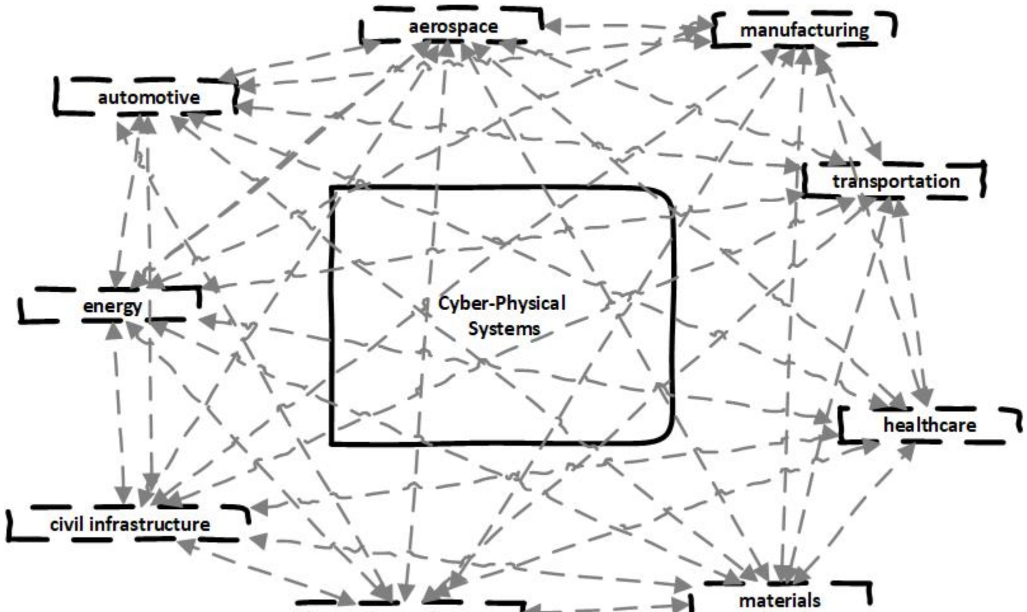

Figure 3.2: Applications of Cyber-Physical Systems and their Networking

Digital systems are being increasingly networked with mechanical systems. These areas of application have security requirements, real-time transmission, scalability, availability, and performance in common.

The structure of CPS can best be compared to the layers of an onion. Systems are created and combined into super-ordinate systems by recurrent linkage with other systems and are known as “systems of systems” [27]. CPS are usually not designed as entirely new systems but emerge by networking existing infrastructures with embedded information technology. The performance and complexity of the newly emerging systems become particularly apparent when they are networked between two or more domains. This occurs when a CPS from the energy industry and health application domains is connected and integrated [18].

3.3 Security Assessment for Cyber-Physical Systems

CPS can be found in many different application areas, as shown above. As such they offer attackers a large surface to attack. CPS are extensive systems with varying communication units and users, including not only humans but also machines. The attacks on CPS can directly affect the physical or cyber parts of the process. A physical attack is one that directly tampers with the physical features by, for example, manipulating an implantable medical device by changing the batteries. A cyber attack is one deployed through malware, software, or by gaining access to communication network elements (for example, by faking sensor information) [28].

The complexity of CPS leads to significant challenges in the area of security. Threats and vulnerabilities can be difficult to assess, resulting in new security problems. It is also challenging to detect attacks that originate from multiple CPS components. These attacks need to be identified, tracked and investigated. Technical security solutions, such as security control (for example, cryptography, access control, intrusion detection) are usually used in IT systems. However, it has been shown that the sole dependence on the known mechanisms is insufficient [29].

CPS are thrilling targets for attackers as they process not only simple but also personal or sensitive data. Hence, a company must comply with security regulations and generally applicable laws such as the BDSG, the GDPR, and the IT Security Act. Security is not only related to technical security, but also to organizational security. In addition to technical aspects, processes must also be analyzed and evaluated in terms of security. In order to ensure a high level of security, systems must be analyzed in terms of data security to be able to implement appropriate security measures. Security assessments are used to evaluate processes and systems with regard to data security. This involves determining the level of security and implementing appropriate security measures. The targeted use of security measures generally improves system security. Furthermore, a process is also established that enables regular security assessments to be carried out, thereby enabling weak points to be identified. The challenge here lies in the CPS themselves. CPS have new requirements for security assessments, which have not yet been reflected in the classic models.

Furthermore, attention must be paid to regulations specifically for CPS. To assess and implement security in CPS, their characteristics must be taken into account. Their essential features are high scalability, volatility, and real-time functionality.

3.4 Summary

CPS are systems that create new pools of data and information by networking various sensors and actuators. The direct connection between the physical and digital domain can be observed in various application areas. For example, CPS can be described with the properties hard to soft time requirements, networking inside and outside the system, and high requirements for functional safety, security of access and privacy, and high-cost pressure (see Figure 3.1). CPS offer great potential for attackers. For instance, this can affect system or data security. CPS are also used in system-critical areas (such as the energy industry). A significant aspect is how security, especially data security, can be ensured in CPS. For modeling data security through security assessments, the characteristics of CPS must be considered in order to obtain a more accurate statement for data security. Through this, more targeted security measures can be implemented to achieve the best possible security level. In the following chapter, smart grid, as an application area, is presented in more detail and the challenges and requirements for security assessments are elaborated.

Chapter 4

Smart Grid

The energy sector has undergone many changes and developments in recent years. Increased awareness of the environmental impact resulting from the carbon footprint is driving the search for renewable and alternative forms of energy generation. This, in turn, is reflected in the growth and development of new technologies. The architecture of the energy sector is moving further away from the traditional vertically integrated utility model, as the emergence of multiple sources of injected electricity means that only a decentralized, distributed system architecture can be considered. The rise of the smart grid offers benefits to society, the power industry, customers, and many stakeholders. This chapter presents a smart grid as an example of a CPS application. It offers an overview of smart grids in general, of smart grids in Germany, their legal basis and architecture, the status quo, application example, and the security of such grids.

4.1 Overview

In future smart grids (compare Table 4.1), lots of data will be generated by meters daily and will have to be stored, archived and analyzed. In Germany, the centralization of the whole system of energy supply is ongoing [5]. The conversion of the system into an intelligent one is creating many new opportunities and challenges, of which the change to the reliance on renewable energies such as wind power or solar energy is especially significant [1].

The smart grid infrastructure is used for not only "energy" like smart metering (see Figure 4.1) but also for smart homes and for gas, water and value-added services. The energy supplier (EVU) operates a data platform to connect users,

TABLE 4.1: Energy-Supply: Today — Future

today	**future**
central supply	decentralized supply
bilateral and wholesale trade (local markets)	centralization (regional market)
transfer energy	transfer energy and data
reading of the meter content: once a year (manual)	smart metering: transfer data all 15 minutes

who in this case are producers, consumers and customers. The SMGW is the secure interface and communication unit between a household and the EVU [1].

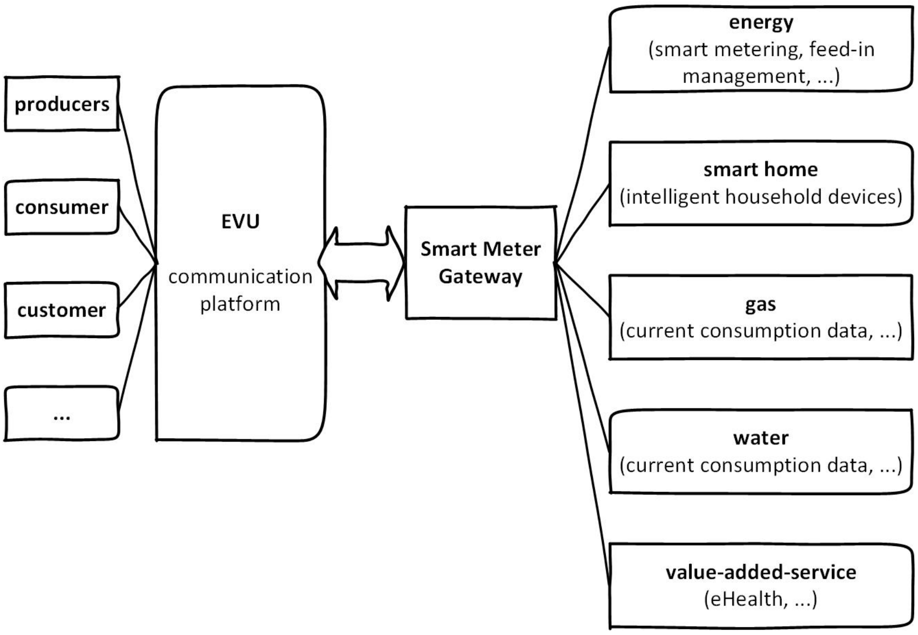
producers
consumer
customer
...
EVU
communication platform
Smart Meter Gateway
energy
(smart metering, feed-in management, ...)
smart home
(intelligent household devices)
gas
(current consumption data, ...)
water
(current consumption data, ...)
value-added-service
(eHealth, ...)

FIGURE 4.1: Application Example Smart Grid

Grids are being converted not only in Germany but also in other European countries. The pioneers are countries like Italy and Sweden [5], and the risks involved in the rollouts are already being assessed. Concerning the security of supply, attacks on control systems of the power grid via the Internet are a growing threat. On the one hand, the power grid can be controlled or manipulated, and on the other hand, confidential data about consumers and their behavior can be accessed. This is because data of varying quality from various sources is processed and analyzed in real-time, so access to the systems must be guaranteed for various groups of people.

The challenges for the smart grid are manifold. Increasing digital processes will raise the computational effort and energy consumption, and the market roles and responsibilities of new players in the trading of electricity are still unclear. Privacy and security must be ensured [30].

4.2 Smart Grid in Germany

This work outlines the conceptual and technical implementation of the smart grid in Germany. Figure 4.2 shows the distinction between a modern measuring system (without communication unit) and an intelligent measuring system (with communication unit) as well as the resulting changes in the transmission of data. The legal framework for the introduction of the smart grid in Germany is already available. The technical guidelines and protection profiles for the SMGW and smart meter have been prepared by the appropriate authority, and a certification procedure has been developed. The market declaration, published on 31.01.2020 [31], was to be the starting signal for the smart meter rollout. Three independent SMGW manufacturers were declared to have successfully passed the certification process, so the rollout can now begin.

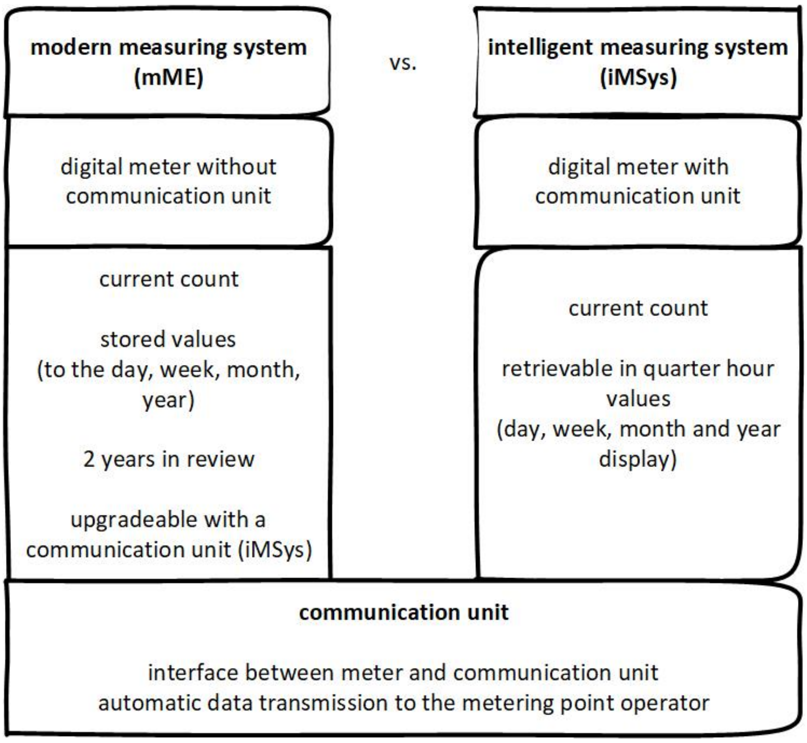
modern measuring system (mME)
vs.
intelligent measuring system (iMSys)
digital meter without communication unit
digital meter with communication unit
current count
stored values (to the day, week, month, year)
2 years in review
upgradeable with a communication unit (iMSys)
current count
retrievable in quarter hour values (day, week, month and year display)
communication unit
interface between meter and communication unit
automatic data transmission to the metering point operator

Figure 4.2: Modern Measuring System vs. Intelligent Measuring System (inspired by [32])

Considering the current state of implementation of the smart grid in Germany, the following points can be clarified: Data and information, trust model, authentication, and requirements for future systems in the smart grid.

- Data and information
  - "*All smart meter data are data worthy of protection*" [6] according to the state conference of data protection officers: all data generated by smart meters or transmitted by the underlying infrastructure (SMGW) is considered as data worthy of protection.
  - Data generator and user — human and machine: data is not only generated by the user as a human being, but also by machines, actuators and sensors.
  - Real-time processing of data (future): in the future smart grid (smart grid 2.0), data processing and access to systems must also be able to take place in real-time.
- Trust model

  - 2-step trust model/security level [8]: in the current trust modeling, the security level secure and insecure are considered.

- Authentication
  - Authentication concept developed by BSI: the authentication concept for the smart grid infrastructure in Germany was developed by the BSI and documented in the corresponding technical guidelines.
  - Customer portal — companies' separate solution: proprietary solutions are used to provide customers with access to their data and consumption values.

- Requirements for future systems for a smart grid
  - High scalability: in the smart grid, a high number of participants and system requests are generated, which can only be observed at intervals.
  - Volatility: smart grid can be described as a network where the number of participants changes by leaps and bounds, rather than the constant number of permanent participants
  - Different types of data: different types of data, such as customer data, power consumption, and IP address, are transmitted, processed and stored.

The challenges and requirements listed above can be observed in the establishment of smart grids in Germany. These points have a direct impact on the security of the smart grid as well as on data security and security assessment.

4.3 Regulatory Framework

The public acceptance of the smart grid depends on whether or not it proves to be safe and private. More and more personal and sensitive data will be processed in these networks in future. With the Energy Industry Act (EnWG) amendment in the summer of 2011, the German government set out to realize smart grids in Germany [33]. Not only the industry-specific laws and regulations but also the generally applicable laws, such as the BDSG, the IT Security Act, and the EU Data Protection Regulation, had to be considered.

In this thesis, the relevant regulatory framework (such as in Figure 4.3) conditions for information security and data protection will be examined. The conditions identified are included as non-functional requirements for the system being developed. The following presentation reflects the status as of March 2021.

4.3.1 Energy Industry Law

The first principles for implementing smart grids were laid down in the EnWG amendment in the summer of 2011 [33]. The implementation of an intelligent

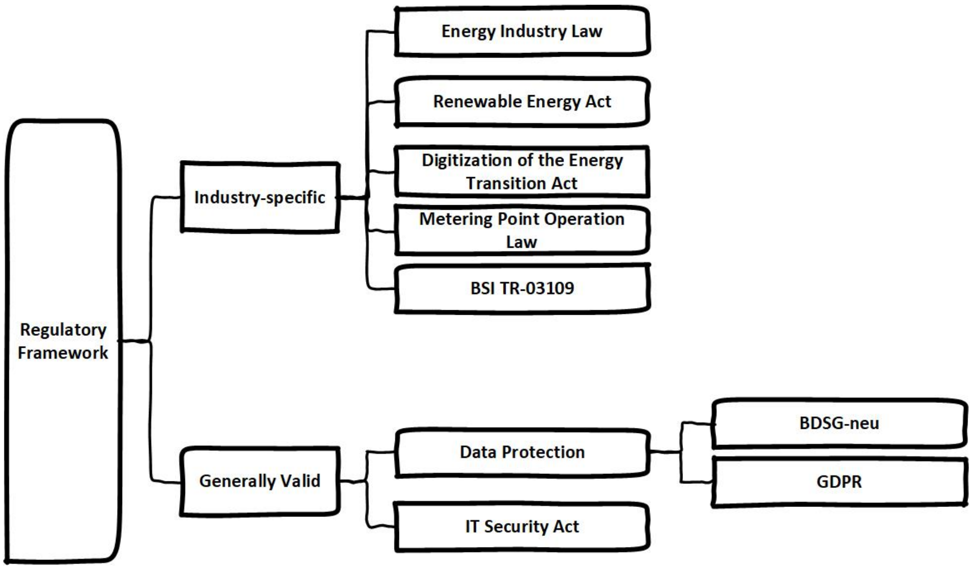

FIGURE 4.3: Overview Regulatory Framework

metering system was enshrined in the EnWG in 2011. According to the EnWG from 2011, sensors must be installed to record the network situation — if required by the consumption and load structure in the corresponding network area — to let the network be intelligently used and controlled if possible. This includes establishing an appropriate IT infrastructure for processing the data and information [34].

In the context of 21e EnWG, we must consider what a metering system is or should be. It is a system of smart metering as a whole. It includes the gateway, the communication link and all the system's components. Section 3 requires that the entities involved in data transmission ensure data protection and data security. In particular, the measures must ensure that data is confidential and unchanged and that the transmitter can be identified.

4.3.2 Digitization of the Energy Transition Act

With the passing of the “Digitization of the Energy Transition Act“ in 2016, nothing stands in the way of the introduction and establishment of smart grids, smart meters, smart metering, and smart homes in Germany. The focus here is on the introduction of smart metering systems. In addition to costs and benefits, key aspects include the minimum technical requirements for ensuring data security and privacy [35].

Chapter 3 contains the technical requirements for ensuring data security and privacy when using smart meter gateways. Article 19, General Requirements for Metering Systems, concerns data privacy, data security, and interoperability in the systems to be used, ensuring that the principles of security and data protection are implemented.

4.3.3 Renewable Energy Act

The expansion of renewable energies is an essential element of the energy transition and is ensured by the Renewable Energy Act (EEG). As renewable energies are increasingly being used, feed-in management (compare § 14 EEG 2017) will play an essential role in future energy grids.

This law does not include any requirements for privacy and data security in the case of communication systems.

4.3.4 BSI TR-03109: Technical Specifications for Smart Metering Systems and their Secure Operation

The requirements for the secure use of smart metering systems were developed as part of the technical guideline (BSI TR-03109). Purely functional specifications were developed for the components in a smart metering system. The security requirements defined in the protection profile for SMGW were specified in more detail [36].

4.3.5 Metering Point Operation Law

The Metering Point Operation Act (MsbG) created the role of the smart meter gateway administrator (SMGWA), who is responsible for the installation and configuration, data reception and monitoring maintenance of a smart metering system. In principle, administrators work for the metering point operator (basic or competitive). The use of personal data is subject to strict legal regulations, so smart metering systems must meet the requirements in Sections 21 and 22 MsbG, to protect and safeguard data [37].

4.3.6 Data Protection

The BDSG was revised in May 2018 by GDPR The GDPR aims to establish a single set of rules for data protection throughout the EU. The GDPR follows the principle of privacy by design and by default. The following section looks at the GDPR and the new Federal Data Protection Act. The Federal Data Protection Act was revised in May 2018 by the GDPR.

4.3.6.1 European General Data Protection Regulation

The GDPR has been in force since May 2018 and has replaced the European Data Protection Directive from 1995. The regulation amends national laws on data protection. The GDPR has six general data protection principles, but data protection by design and default is central. The principles are fairness and lawfulness, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality [38]. Essential points in the GDPR are, in addition to more effective protection of privacy, the strengthening of the basic right to informational self-determination. Likewise, the GDPR enshrines uniform rules for processing personal data. Processors must implement Article 32 of the GDPR and ensure appropriate technical and organizational measures.

Here we can focus on Paragraph 32 GDPR security of processing. Article 32 par.1: "*[...]*

- *the pseudonymization and encryption of personal data*
- *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*
- *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*
- *a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing [...]*"

This means pseudonymizing and encrypting personal data, safeguarding the security goals (confidentiality, availability, integrity, and resilience) of the systems in the long term, and a regular review, assessment and evaluation of the effectiveness of technical and organizational measures in the short term.

4.3.6.2 Federal Data Protection Act

The GDPR amended the BDSG. The scope of application was regulated by Art. 1 BDSG. According to Article 2 (1) of the GDPR, the regulation applies to all circumstances in which personal data are processed in whole or in part by automated means, but it also covers situations in which personal data are processed non-automatically when data are stored in a file system [39].

In the context of this thesis, reference is made to Article 64 (3) BDSG-neu. This states that, in the case of automated processing, the controller and the processor must assess risks and take measures

1. to deny unauthorized persons access to equipment used for processing (access control)
2. to prevent unauthorized accessing, copying, changing or deleting of data media (data media control)
3. to prevent an unauthorized input of personal data as well as unauthorized knowledge, modification and deletion of stored personal data (storage control)
4. to prevent the use of automated processing systems with the help of devices for data transmission by unauthorized persons (user control)
5. to ensure that persons authorized to use an automated processing system have access to only the personal data covered by their access authorization (access control)

6. to ensure that it is possible to verify and establish to which entities personal data have been or may be transmitted or made available through transmitters (transmission control)
7. to ensure that it can be checked and established retrospectively which personal data have been sent into or modified by automated processing systems, when and by whom (input control)
8. to ensure that the confidentiality and integrity of data are protected during the transmission of personal data as well as during the transportation of data carriers (transport control)
9. to ensure that systems deployed can be restored in the event of a fault (recoverability)
10. to ensure that all functions of a system are available and that any malfunctions are reported (reliability)
11. to ensure that no personal data stored can be harmed by system malfunctions (data integrity)
12. to ensure that personal data processed on behalf of a client can be processed only following the client's instructions (order control)
13. to ensure that personal data is protected against destruction or loss (availability control)
14. to ensure that personal data collected for separate purposes can be processed separately (separability)

4.3.7 IT Security Act

The aim of the IT Security Act, passed in July 2015, was to increase the security of information technology systems. It was meant for operators of web offers, telecommunications companies, BSI, and operators of critical infrastructure such as the energy industry. The main requirements of the IT Security Act are the establishment and operation of a reporting system for significant disruptions to critical IT systems and compliance with the minimum security level of IT systems. One requirement relating to the smart grid is the minimum security level regulated in §8a BSIG. Operators of critical infrastructure must ensure that IT security is "state of the art" and regularly show this to the BSI. The IT Security Act regulates so-called minimum standards, which stipulate minimum levels of security of information. In addition, the obligation to report is enshrined in law in Section 8b BSIG: "Central Office for Critical Infrastructure Information Security". The BSI is the central reporting office for operators of critical infrastructures in security matters in information technology. It concerns operators of critical infrastructures specified by the BSI Act in terms of the threshold values set out in the BSI Criticality Ordinance. Significant disruptions to the availability, integrity, authenticity, and confidentiality of IT systems, IT components, and IT processes must be reported if they have or may have harmed critical infrastructure. A prompt message is always required [40, 41].

4.4 Architecture — German Approach

The reference architecture of a smart grid consists of the Local Metrological Network (LMN), the Wide Area Network (WAN) and the Home Area Network (HAN). Communication takes place through the SMGW, and the existing architecture is extended with IoT devices for new applications and services. The IoT architecture consists of a device or sensor connected via a gateway to the router and the Internet. The collected data is stored centrally on a server and is available to users if required. Figure 4.4 shows the unification of the architecture of a smart grid and IoT (smart grid 2.0) [8].

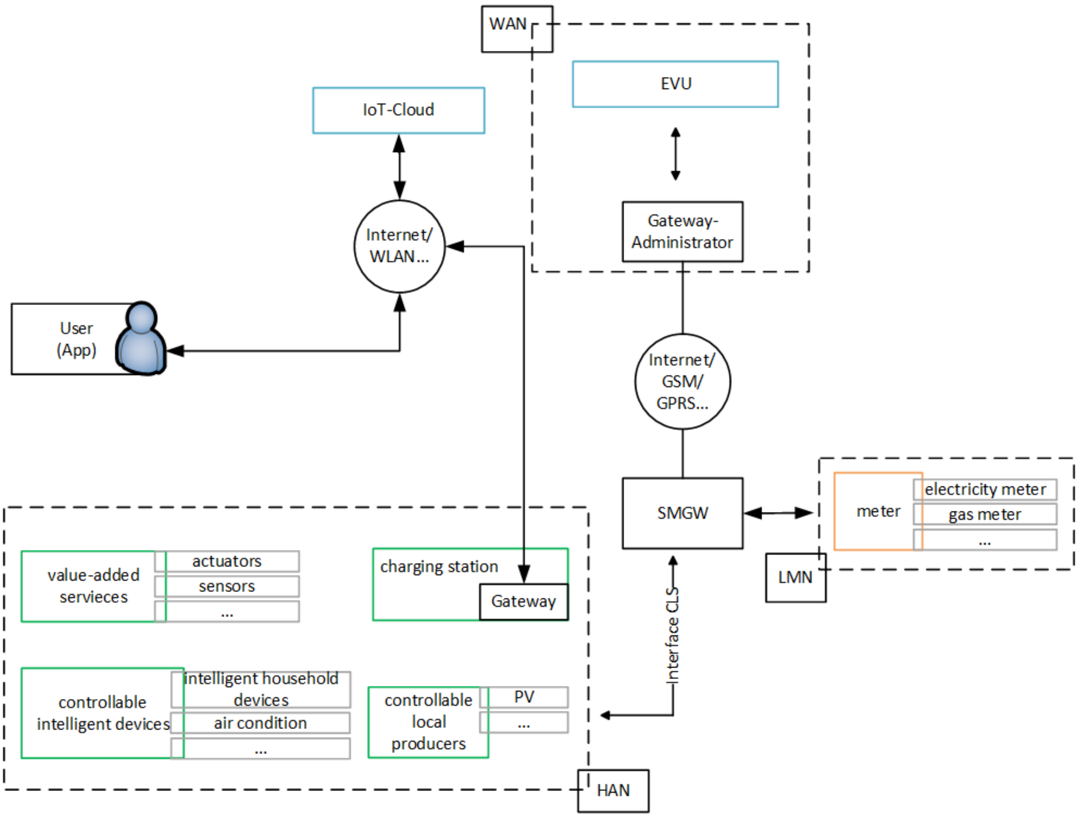

FIGURE 4.4: Architecture Smart Grid with IoT

Authentication

Requirements crucial for security must be fulfilled by future systems in a smart grid. In the following, we will look at the technical implementation with regard to authentication. The focus here is on smart metering in Public Key Infrastructure (PKI) in accordance with Technical Guideline TR-03109 [42], which is deemed to be state of the art in Germany.

Smart Metering in PKI by BSI

SMGW is linked to authorized market players in the WAN (secondary network) only with mutual authentication of the communication partners. The data are encrypted and signed by the SMGW at the data level for the end recipient. The PKI model chosen has a central, governmental root for the trust anchor of the gateways. Private companies operate as sub-CAs, responsible for servicing market players [43]. The technical realization of the certificates is proceeding in the form of X.509 certificates. In addition to the smart metering certificates, there are LMN certificates and HAN certificates. The LMN certificates can be used for mutual authentication of meters and SMGW in the LMN. They are self-signed and not from the smart metering PKI. The HAN certificates can be used to authenticate devices at the HAN interface of the SMGW [42].

Discussion
According to BSI, the smart metering of PKI together with the requirements for future smart grids and information security and data protection is under consideration. Questions have arisen about the performance, certification, update management, security, number of participants, and the security level achieved.

Performance: The number of certificate checks increases if we consider the smart grid 2.0, increasing the number of participants and services communicating via the smart meter gateway. These certificate checks have an impact on performance.

Certificate Management: As the network grows, the number of participants holding a certificate increases. This also increases the effort needed for certificate management, consisting mainly in the management, validity, verification and issuance of certificates.

Update Management: In the case of update management, the question arises as to whether this also works for highly scalable, volatile systems, when many certificates have to be adapted or exchanged.

Number of Participants: The existing PKI infrastructure must map a high number of participants in the future system. Participants can be assigned to different areas or different roles and may be either people or devices.

Level of Security: The smart metering of PKI tries to provide maximum security at all levels and for every instance of use. This requirement leads to a complex PKI, which should also be implementable in highly scalable, volatile systems. This raises questions concerning the level of security achieved with the PKI currently in use. Will it still work in the future system, and how can it be optimized?

The analysis of the authentication mechanism in the smart grid has shown that the mechanism will reach its limits in the future smart grid (smart grid 2.0). Challenges are posed by the fact that the grid is highly scalable, volatile and dynamic.

4.5 Actors and Roles

The influence of information and communications technology and the energy transition has given rise to new business processes, digital services, and services in the energy market. In this development, new market roles and players with various functions and authorizations are emerging. The previous identity management must be adapted and further developed. Stakeholders in today's energy market are: generators (including virtual power plants), (distribution) grid operators and balancing coordinators, meter operators, wholesalers (balancing group managers) as well as retailers (suppliers and balancing group managers), prosumers, and end consumers. In addition to these traditional players from the energy sector, there will also be infrastructure providers, platform operators, and service providers at the interface to the end consumer [21]. Many roles and actors in a smart grid are already known. Furthermore, new cases of uses and technological developments will create more players and roles.

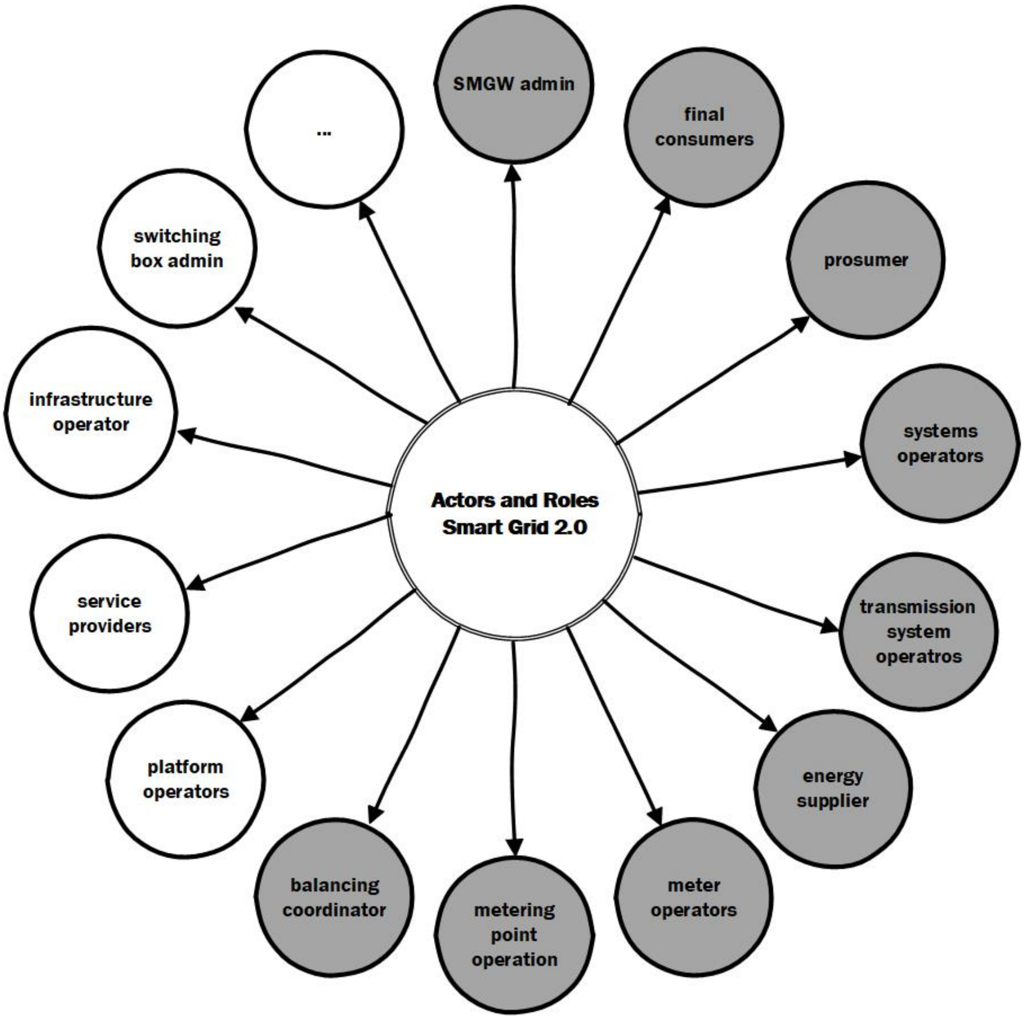

FIGURE 4.5: Actors and Roles in the Smart Grid 2.0

Figure 4.5 shows an overview of roles and actors in a smart grid. The lighter icons represent future roles to be further defined and specified. Explanations and definitions of the known roles and actors can be found in literature [6], [35], and [34]. For example, the "switching box administrator" is thought to be a new future role. He will administrate the switching operation in the network.

4.6 Application Example

The following subsections present the cases of use considered in the context of this thesis. Such cases are assigned to the areas "known", "in preparation", and "future". The cases smart metering ("known"), feed-in and load management ("in preparation"), and value-added services ("future") are described. These application examples are the basis for the "smart grid" case study in Chapter 7.5.

4.6.1 Smart Metering

The "smart metering" case of use can be described as a classic case from a smart grid. In the future smart metering system, electricity consumption will no longer be read manually once a year but automatically at specific intervals (for example, every 15 minutes). For this purpose, each household will be equipped with an iMSys consisting of a base meter and SMGW. The prerequisite for receiving or retrieving the measured values is the registration and configuration of the meter in the SMGW [36]. The configuration of a meter, however, lies outside the scope of this thesis. Figure 4.6 shows a classic infrastructure in which a smart meter and an SMGW are present at the consumer. In addition, the system architecture at the grid control center is shown.

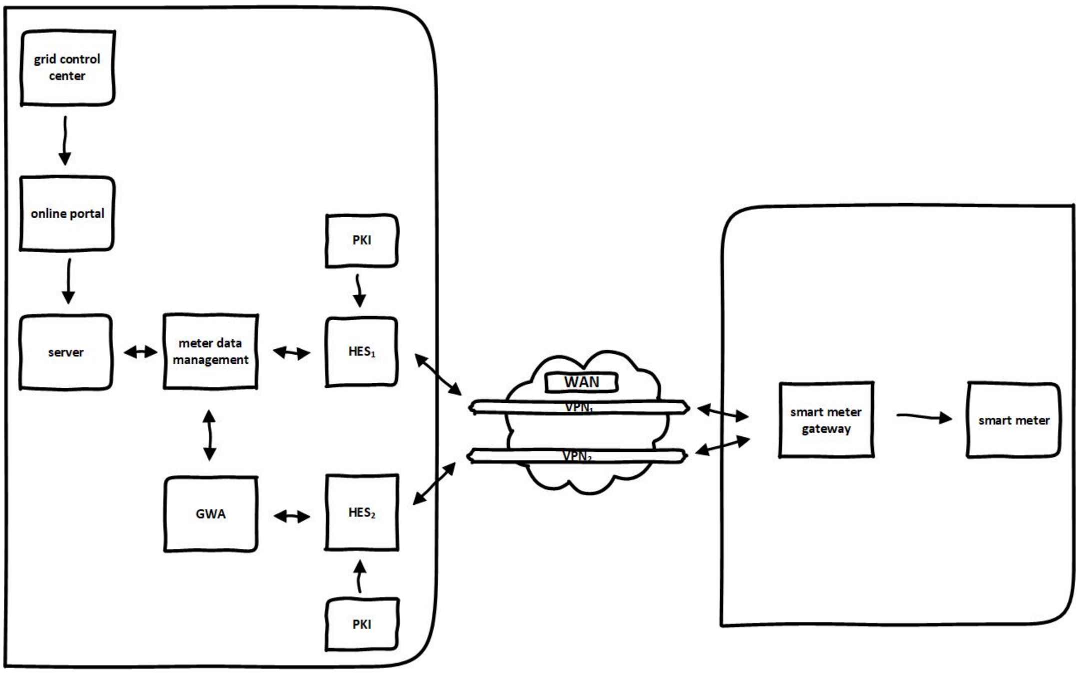

Figure 4.6: Architecture Smart Metering

The processes described below represent the essential processes in smart metering and will be used further in this work. The first process is the registration of the smart meter. The unit to be registered must identify itself to the network provider, which is implemented in the form of device and customer ID. In addition, the network provider must assign this identity to an SMGW, so the IDs must also be transmitted. The second process represents the opposite operation of the first process. It is the deletion of the smart meter from the consumer. In order for the network provider to uniquely identify the smart meter, the IDs described above are also used. In the smart metering environment, it must be possible to update the software of the meter used: to change system settings and to be able to perform security updates. In the third process, two different scenarios must be considered. The first scenario involves a group of devices that can be attributed to exactly one user. The second scenario, is an update for several or, if necessary, all users. Process 4 describes the reading of the values. This means how much energy a consumer has consumed, which is done in 15 minutes intervals.

4.6.2 Feed-In and Load Management

According to the Renewable Energy Act (EEG Art. 6), operators of renewable energy systems of up to 100 KW must grant the grid operator some intervention options to reduce the feed-in power. In return, the operator is obliged to carry out an accurate registration and recording of the EEG management measure. Furthermore, it must compensate the plant operators affected for the electricity not fed into the grid. As an example the grid area of Bayernwerk can be considered, for which 1,007 rule sets were necessary in June 2014 [44]. For this purpose, data from the plant operator is stored at the network operator and must be analyzed and processed. In addition, further data are generated daily by the intelligent energy supply system and stored. A result of the data analysis may lead to the shutdown or connection of generation or consumption plants, which means intervening in the security of supply. The difference between the energy fed into the grid and the energy consumed is determined every 15 minutes. If there are deviations, energy is used to balance them out. Control energy is provided by connecting and disconnecting interruptible consumption devices by Art. 14a EnWG [6]. In this context, there have already been publications that address this problem and see a need for action (compare Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) - traffic light concept (yellow and red phases) [45]).

The Smart Energy Management Program (SEMP) is a publicly funded research project and creates a reference solution for a new type of active management for renewable energy feeders at low and medium voltage levels and large consumers. SEMP comprises a local control unit (SEMP Box) that receives, validates and executes commands via the SMGW, as well as an active SMGWA system for control, billing and compensation management, a system infrastructure, or process landscape for installation, operation and maintenance of the system by corresponding service providers such as grid operators [46].

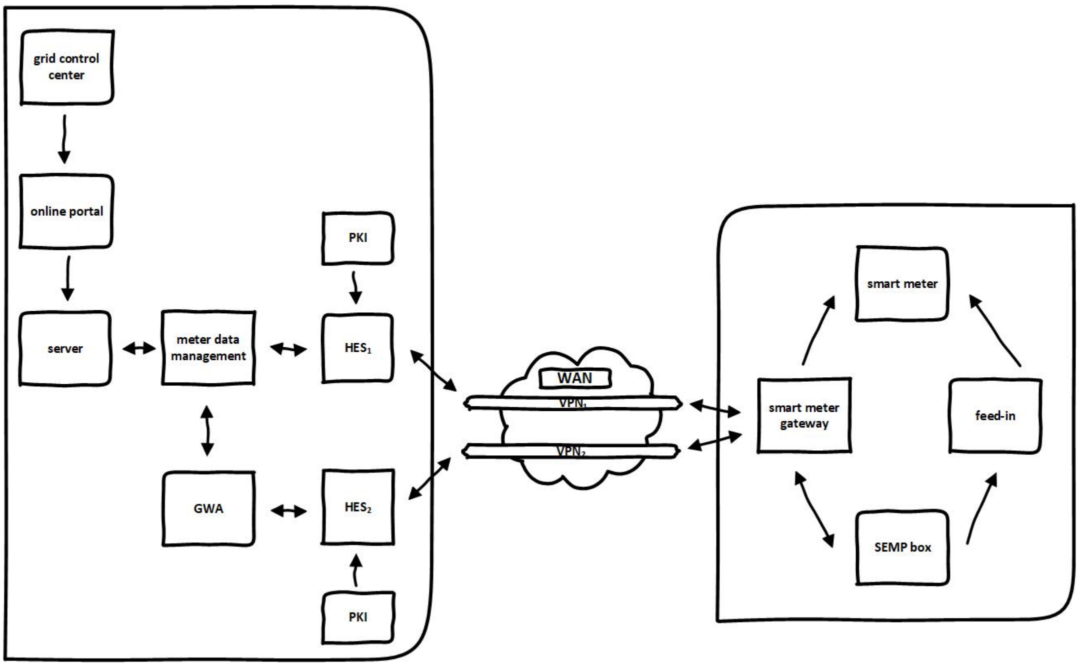

Figure 4.7: Architecture Smart Energy Management Program

The processes shown below represent the essential processes in feed-in and load management at the SEMP project example and will be used further in this work. The first process is the registration of the switching box (SEMP box). In this process, the unit to be registered must identify itself to the network provider, which is implemented in the form of a device and customer ID. In addition, the network provider must assign this identity to a smart meter or SMGW, so the IDs must also be transmitted. The second process represents the opposite operation of the first process. It is the deletion of the switching box at the feeder. In order for the network provider to uniquely identify the switching box, the IDs described above are also used. In the feed-in and load management environment, it must be possible to update the software of the devices used. Primarily, to be able to change system settings and to perform security updates. In the third process, two different scenarios must be considered. The first scenario involves a group of devices that can be attributed to exactly one user. The second scenario is an update for several or possibly all users. The fourth process involves the registration of the system as a whole. For the registration of the system with the network operator, the necessary IDs (compare with process 1) are required. Similarly, process 5 describes the deletion of the system or the plant. Process 6 involves the reading of the values. This means how much energy is fed into the grid. In process 7, the execution of measures is considered. With measures is to be understood, how much energy can be fed into the net. This means a reduction in the amount of energy fed into the grid or the addition of power to the grid.

4.6.3 Value-Added Services — Secure Gateway Service for Ambient Assisted Living

The Secure Gateway Service for Ambient Assisted Living (SEGAL) is a publicly funded research project and is an example of a value-added service. Digitization is making it possible to increase network applications and processes in the energy industry. With the help of sensors and actuators, devices can be controlled or administered almost without human intervention. The necessary communication infrastructures have already been developed for the smart grid. The focus here is on the secure exchange of standardized data and information. The design of this communication system entails new possibilities in other areas as well. Thus, not only energy-related services can benefit from the infrastructure. In the area of value-added services, such as AAL, new possibilities are opening up. Within the scope of this project, an information technology solution approach is to be developed, which communicates via the IT infrastructure of the energy sector (SMGW). Through the "secure channel", which is already present in all households (or will be in the future), sensitive and personal data of persons in need of assistance will be transmitted, for example, to provide assistance to the care service. The areas of application can be divided into the categories of building surveillance, movement monitoring, body-related sensors and emergency buttons [47].

The project aims to develop a SEGAL service based on AAL devices (IoT devices) and a smart grid. 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.), and smart home devices (smoke detector, thermostat, etc.). The communication occurs via an SMGW connected to the AAL hub, which connects the sensors, manages the correspondence with the gateway, and aggregates the resulting data [9].

The first component is the integration layer for sensor technology. This is where data is collected from sensors or manual inputs. Manual inputs are, for example, the confirmation button for the nursing service or the triggering of a fire alarm. The integration layer is intended to serve as a meta-level for connecting the sensors. The next system component is the so-called AAL hub. Here, the collected data from the sensors is temporarily stored, aggregated and analyzed in terms of security. After the data has been analyzed in the AAL hub, it must be sent via a secure communication infrastructure. This is what the SMGW is designed to ensure. It is the interface between the AAL hub and the remote control center. The aggregated data from the AAL hub is evaluated and documented here. If an anomaly is detected in the AAL hub, resulting in an emergency call, this is forwarded to the responsible institutions in the remote control center to guarantee the fastest possible assistance [47].

The processes shown below represent the essential processes in SEGAL and

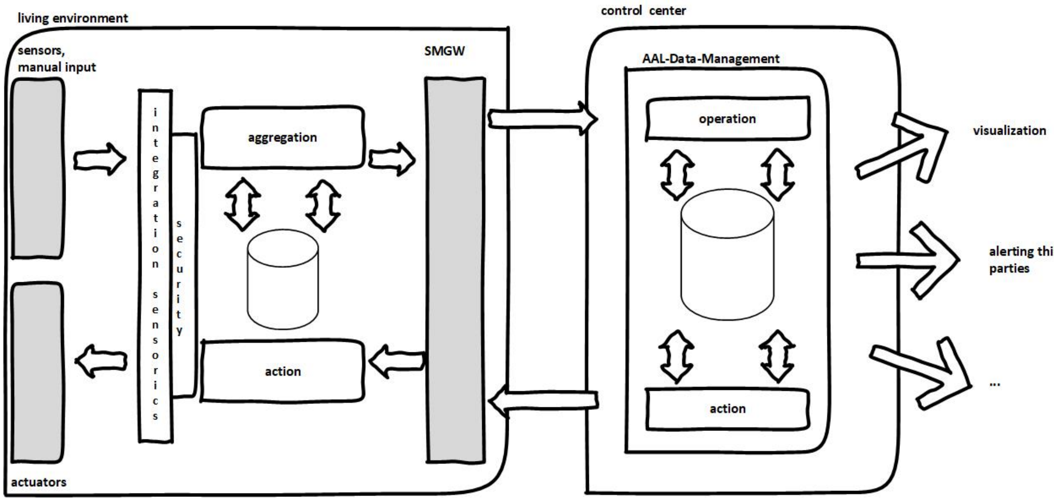

FIGURE 4.8: Architecture Secure Gateway Service for Ambient Assisted Living

will be used further in this thesis. The first use case is the initialization of a unit at the end user. A unit can be a sensor or actuator as well as a new end device that is connected to the service. The unit to be registered must identify itself to the AAL control center, which is implemented in the form of a device and customer ID. In addition, the control center must assign this identity to an AAL hub, so the hub ID must also be transmitted. The second use case is the opposite operation of the first use case. It is the deletion of a unit at the end user. So that the AAL control center can uniquely identify the unit, the IDs described above are also used. In the AAL environment, it must be possible to update the software of the devices and sensors used, since it is assumed that the person being cared for is not capable of keeping the described infrastructure up to date. This can prevent security risks. In the third use case, there are two different scenarios to consider. The first scenario involves a group of devices that are attributable to exactly one user. In this use case, the AAL control center must use the hub ID and the device and customer ID to locate the device in question that requires an update. The second scenario is an update for several or possibly all users. This should correspond to a firmware update of the AAL hub. It is therefore recommended or mandatory for all users. The transmission of diagnostic data from physicians or information for care services is considered in the fourth use case. This involves sensitive data, where personal data can be tapped with reference data. The fifth use case is the transmission of emergency data. Here, emergency data is characterized by the fact that it contains irregularities or indications that suggest that the person being cared for needs immediate help. An example of this would be when a pacemaker provides unusual values suggesting that a health risk is imminent. The transfer of analysis data is the sixth and final use case. This concerns data collected by the sensors. Often, this data has no personal reference from the outset, but if this is the case, it is anonymized and is only used for analysis purposes.

4.6.4 Summary

A clear line must be drawn between the data transmitted and, if necessary, stored and processed and the data already stored. This includes the following identified data, which are transmitted and, if applicable, stored and processed: Tariff profile data, end consumer credentials, consumption data, feed-in and feed-out quantities, metering data, billing data, invoice amount, voltage, frequency, phase angle, gateway ID, gateway key, gateway certificate as well as gateway status data, IP address, updates and patches, authorization profile data, time, list of all assigned meters and their credentials, list of metering point operators for each meter, data, and information from value-added services, data and information from the water and gas sectors. The data stored (for example, at the utility company) are customer or classic master data.

4.7 Security Requirements

The regulatory framework, architecture, actors and roles, and an application example of functional requirements for the system for processing and storing information transmitted via the IT infrastructure of a smart grid have been outlined. Non-functional requirements for security systems in a smart grid are:

Confidentiality
The confidentiality of data and information must be ensured. Data and information or access to systems should be available to, or obtained by, only authorized persons. The confidentiality of data and information for future smart grids means protecting personal or sensitive data. This applies not only to the system level but also to the data level. The bottom level — data level — must ensure confidentiality. This can be done by protecting the data itself. A technical possibility consists in encoding the data according to the level of protection desired. Confidentiality also includes controlling access to the system. A distinction is made between authorized and unauthorized access. The technicalities can be implemented with suitable authentication mechanisms.

Availability
Availability means that the data and information must be made available according to the legal regulations. The system must be accessible [21]. In terms of the availability of data and information in smart grid 2.0, it must be possible to retrieve data every 15 minutes in smart metering (compare EnWG). All other data and information will be handled in various ways, depending on the respective policies of the companies. To achieve this in a dynamic, volatile system, authentication mechanisms must be in place.

Integrity
The integrity of the data and information has to be ensured by preventing falsification. When considering the integrity of data and information in smart grid 2.0, it must be ensured that any changes to data can be traced. Furthermore, it must also be possible to differentiate between accesses. This requires apt

identity management and a mechanism of authentication to make this possible.

Furthermore, it must also be possible to differentiate between accesses. This requires appropriate identity management and an authentication mechanism that makes this possible.

Obligation
Authenticity and non-repudiation are obligatory for protection [21]. In smart grid 2.0, this means that the receipt of data and information during transmission should be indisputable as the source of information (for example, a smart meter). The authentication mechanism used must enable this through suitable procedures.

Further non-functional requirements, which will not be further mentioned, are: anonymization and pseudonymization, reliability, non-linkability, transparency, intervenability, and purpose limitation.

The non-functional requirements presented here can be considered as requirements for security assessment. By considering and evaluating these non-functional requirements, the security of the system is ensured.

4.8 Summary

The digital transformation of the energy supply to an intelligent energy supply system is creating numerous new opportunities and challenges. In the smart grid, large amounts of data are generated daily during the reading of meter data. The underlying infrastructure (SMGW) is being opened up for further applications, right up to unification with smart home technology. As a result of this increase networking, the original idea of the smart grid is also evolving further into a smart grid 2.0 with new challenges and requirements. These challenges can be seen in the previously valid trust model and in the real-time requirement. Due to the high volume of data with different origins and quality, the question arises whether this trust model still meets the future needs of smart grid 2.0. The other requirements for the smart grid 2.0, which can also be related to CPS, are high scalability, volatility and different types of data. The security requirements of the smart grid are the classic goals of data security with confidentiality, availability, integrity, and obligation. But how can these goals of data security be guaranteed, considering the new requirements of smart grid? Are the existing process models for security assessment with the criterion of data security still suitable and do they have to be extended by the new requirements? If the aspect of data security is considered in isolation, the currently valid trust modeling must be analyzed.

Chapter 5

Problem Statement

Security in CPS generally describes the research context of this thesis. CPS can be described as highly scalable and volatile systems. The smart grid is an example of a CPS in this thesis. One challenge here is the security assessment in these systems. For CPS in general and the smart grid in particular, it is necessary to develop a procedure model that enables security assessments under the underlying conditions of CPS. This chapter examines the starting position of CPS and the smart grid. Furthermore, the research question is posed.

5.1 Starting Position — Status Quo

CPS can be described as systems in which the system boundaries are blurred. They represent a network between the physical and digital worlds. CPS are further characterized by the fact that users or participants in these systems can be both humans and machines. A wide variety of sensors and actuators interact (see Chapter 3). CPS, in the context of security, means new challenges and requirements in analysis and evaluation. CPS are not comparable with conventional systems or structures, so there is a gap in current frameworks for security assessment. Known frameworks and approaches were developed for systems with different characteristics. Security is an important sub-area in CPS, as CPS are used in various critical infrastructures. One application area of CPS is smart grids (see Chapter 4).

Figure 5.1 shows an overview of a smart grid. The key part of a smart grid's infrastructure is the SMGW. This is the secure communications equipment for the data transfer. The application fields, for example, are

- energy — smart metering
- a smart home — the control of intelligent household devices
- gas — data exchange of the current consumption
- water — data exchange of the current consumption
- a value-added service — a health service

There are also users like producers, consumers, and customers. The data exchange takes place via the communication platform owned by the energy supplier.

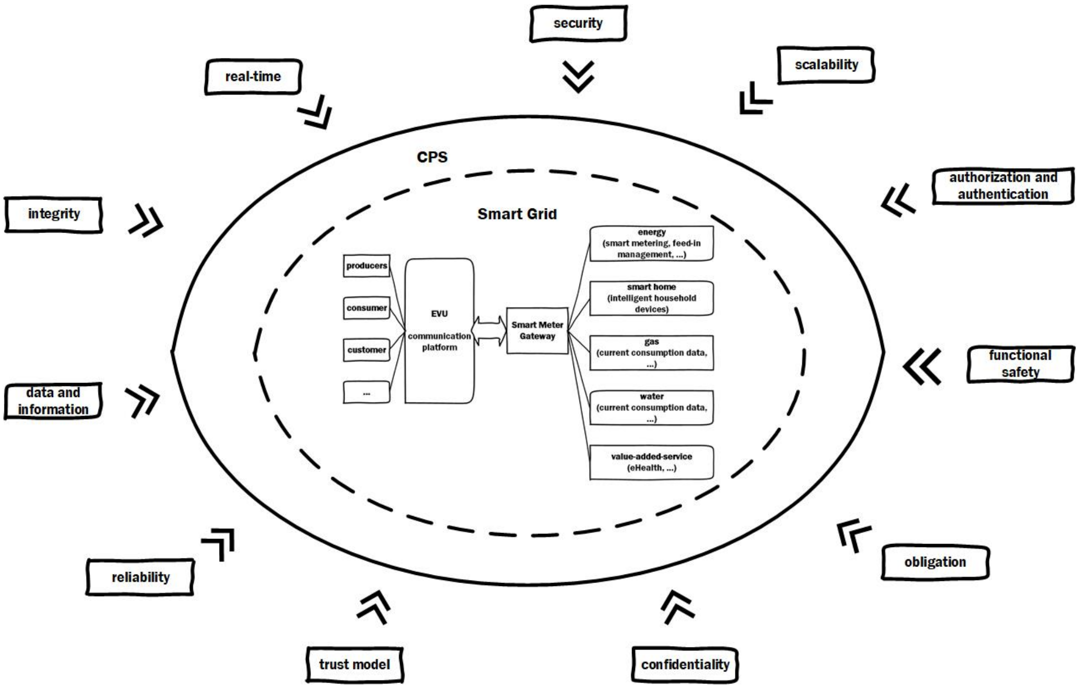
security
real-time
scalability
integrity
authorization and authentication
CPS
Smart Grid
producers
consumer
customer
...
EVU
communication platform
Smart Meter Gateway
energy (smart metering, feed-in management, ...)
smart home (intelligent household devices)
gas (current consumption data, ...)
water (current consumption data, ...)
value-added-service (eHealth, ...)
functional safety
data and information
reliability
obligation
trust model
confidentiality

FIGURE 5.1: Status Quo: Cyber-Physical Systems and Smart Grid

As explained in Chapter 4, in addition to security, there are also challenges concerning data and information, trust model, and authorization and authentication. The current status is described below.

Data and Information

"*All smart meter data are worth protecting*" (the national conference of data protection officers in Germany) [6]. Basically, all data and information are worth protecting. The data generators and users are humans and/or machines, and the processing takes place in real-time.

Trust Model

The trust model has two levels, so data are both secure and insecure [8].

Authorization and Authentication

The federal office regulates the authorization and authentication of a smart grid to ensure information security (BSI). In the case of a customer portal like an energy portal, companies have their own solutions.

From Chapter 4 and the current status presented above, characteristics of future systems in a smart grid can be derived, which are described below.

CPS — Characteristics of Future Systems in a Smart Grid
A smart grid is a variant of CPS. These future systems will be typically highly scalable and volatile and will have to cope with a high volume of data and various kinds of data. The use case data logging "electricity" has the characteristic of being highly scalable. What is shown is the flow of data from final consumers to the energy supplier. Two million participants equal 192 million consumption values per day if the volatile data is transferred once every 15 minutes. Here, the communication in the use case data logging "electricity" is considered. Another characteristic is "high data volume". For example, there are two million participants and 22 gigabytes of data in the use case data logging "electricity". These data are of various kinds, such as customer data or data about power consumption, the IP address, etc.

5.2 Research Objective

The research context of this thesis addresses information security for CPS in a smart grid. To meet the requirements of information security and data protection in highly scalable and volatile systems (CPS), the previously valid trust model must be developed further to cope with the future flow of data and thus reduce complexity. What frameworks can be used to ensure information security through new security modeling for CPS?

This thesis aims to adapt conventional models for security assessment in CPS and absorb requirements more equitably. A security assessment framework is developed based on the necessity for security assessment in CPS. Security measures must also be considered in a needs-based security assessment. Based on the example authentication, security measures are evaluated. The aim here is to clarify how security measures can be assigned to the security assessment. The developed framework will be validated on the practical example of the smart grid, and the application will be shown in practice.

The aim of this thesis is to investigate CPS with respect to security assessment. The central issue is whether the known security assessment methods can be applied to CPS and to provide a complete statement regarding security. Classical security assessment procedures only use the criterion "data security" for security assessment. In the case of CPS, consideration of solely the security criterion is no longer sufficient. Additional criteria must be applied. The additional criteria are derived from the CPS requirements analysis. In the context of this work, the additional criteria of scalability and real-time are considered.

The extended security assessment is performed using a process-based approach. The system (compare CPS) is divided into its processes and analyzed based on the evaluation criteria concerning data security, scalability, and real-time. Known process models are not based on a process-based approach. The model developed in the following chapter can be seen as a holistic view of security assessment. In addition to modeling for security assessment, a procedure for evaluating measures is also presented. The measures must also be classified with regard to the criteria of data security, scalability, and real-time requirements. The model developed can be automated. It should be possible to perform automated security assessments in CPS and show the corresponding measures.

As further side findings, the interaction between data security, scalability, and real-time will be evaluated. What is the relationship between these three criteria, and how do they influence each other? The innovation can be seen in the adapted and need-based security assessment for CPS. A procedure model for security assessment is developed which meets the characteristics of CPS.

The process-oriented approach can be seen as a further innovation. A security assessment of the processes that are mapped in the CPS takes place. In addition to the process-oriented assessment, further criteria can be seen as a new approach. In the context of this work, security assessment is extended to include the criteria of scalability and real-time.

The procedure for developing the process model for security assessment first includes the requirements analysis. As part of this, the smart grid application field is also examined in addition to CPS. Within the scope of the requirements analysis, the known security assessment procedures are considered regarding their application to CPS. Derived from the requirements analysis, the definition of the requirements for the security assessment of CPS takes place using the example of a smart grid. Based on the defined requirements, a holistic, process-oriented framework for security assessment in CPS is developed. The evolved framework is demonstrated using the smart grid application and the authentication measure example based on an empirical study. The added value of the framework for the smart grid is shown, and the applicability in other areas is displayed using the automotive example.

This procedure describes the development and testing of a process-based framework for security assessment in CPS. The goal is to perform the security assessment of CPS in an application-related manner and tailored to the needs using a process-based framework and thus to conduct security investigations automatically. On the one hand, the framework should be able to make statements about security, considering further criteria (real-time requirement, scalability). On the other hand, the corresponding measures, which have also been classified, are selected according to the security assessment. The principle of needs-based security should apply here.

Chapter 6

Requirements Analysis Security Assessment

For the development of a new process model for security assessment in CPS, a requirements analysis must be carried out. The goal is to identify all relevant requirements for the model development. This chapter presents the requirements' analysis for the development of the security modeling, assessment, and measures. In this context, state of the art is considered in terms of security modeling and assessment. Furthermore, the requirement for security modeling and assessment with CPS is derived and defined.

6.1 Related Work — Security Assessment

State-of-the-art models, approaches and frameworks are examined by posing the following question: Which approaches or frameworks are available for security modeling for highly scalable, volatile systems or CPS? An overview of the current state of science and the best practices for security modeling in this area is provided in the following outline.

- Best practice — BSI, ISO/IEC 27000 or ISO/IEC 29100:2011(E)
- Scientific publications — security and privacy by design, security patterns
- Security and risk assessment in CPS

Selected models, approaches and frameworks are examined below and analyzed in terms of CPS requirements.

6.1.1 BSI-Standards

The German Federal Office for Information Security (BSI) Standards describe methods and procedures for various information security topics.

- BSI-Standard 200:1: general definition of the requirements for an information security management system
- BSI-Standard 200:2: presentation of the IT-basic protection methodology
- BSI-Standard 200:3: presentation of risk management [48]

BSI standards 200-1, 200-2, and 200-3 have replaced the BSI 100-X series standards since October 2017. In addition to the standards, the IT-Basic Protection Compendium has been developed and contains the IT-basic protection building blocks. Here, the threats and security requirements are described in each case. The compendium contains concrete recommendations for implementing the IT-basic protection methodology [48]. The main component of an information security management system is security modeling. BSI security modeling is described in BSI Standard 200-2.

BSI-Standard 200-2: IT-Basic Protection Methodology
BSI Standard 200-2 describes the classification of information. An assessment of protection requirements is used to determine what protection is sufficient and apt for the business processes, the information thereby processed, and the information technology used. For each application and set of information processed, the harm expected in terms of confidentiality, availability and integrity is considered and assessed. Here, the data (information), rooms, communication links, and IT system are examined and assessed for the sake of finding ways to protect them. The security level is defined as follows.

- normal — the harm done is limited and manageable
- high — the harm done may be considerable
- very high — the harm done may be catastrophic

The following harm may occur if the primary goals of information security are lost:

- breach of the laws, regulations, contracts, etc.
- impairment of information and rift of self-determination
- impairment of personal integrity
- impairment of task performance
- negative internal or external effects
- financial effects

The first step in assessing the protection requirements is to determine the protection requirements of the business processes and applications; the second step is to determine the protection requirements of the individual objects (for example, IT systems, rooms, and communication links), and the third step is to apply the protection requirements to the applications and systems (comparing the maximum principle, cumulative effect) [49].

6.1.2 International Organization for Standardization

The International Organization for Standardization (ISO) was founded in 1946. Since then, more than 22.000 standards have been published. The ISO Norms are recognized in the industry and are regarded as norms even outside Germany [50]. The following describes the ISO/IEC 29100 and ISO/IEC 27100.

6.1.2.1 ISO/IEC 29100:2011(E): Information Technology — Security Techniques — Privacy Framework

In the context of the ISO/IEC 29100 standard, the following privacy principles are described [51]:

- consent and choice
- purpose legitimacy and specification
- collection limitation
- data minimization
- use, retention, and disclosure limitation
- accuracy and quality
- openness, transparency, and notice
- individual participation, and access
- accountability
- information security
- privacy compliance [51]

This standard includes no security models or assessments but includes principles on how to handle data and information.

6.1.2.2 ISO/IEC 27000: Information Security Management Systems

The ISO 27000 series describes an information security management system (ISMS) comparable to BSI basic protection. It also includes a framework for security modeling. This standard is used in medium-sized and large companies [52] and includes

- requirements for an ISMS and for those who certify and define such systems
- direct support, detailed guidance and/or interpretation for the overall process
- requirements for the establishment, implementation, maintenance, and improvement of an ISMS
- sector-specific guidelines
- conformity assessment for ISMS

Information, infrastructure, rooms, etc. are analyzed and evaluated, and protective measures are derived, as in the modeling of BSI security.

6.1.3 Dimension-Relational Organizational and Problem-Based Security Model

The dimensionally relational organization and problem-based security model (DROPS) is a model of information systems security that makes it easier to identify security requirements and optimal alternative actions in the form of apt security measures. The underlying approach of DROPS is holistic and extensible. Here, security considerations in connection with information systems are not limited to a technical perspective (IT security) but include the integration of non-technical system components (for example, personnel system components). Non-technical security measures (for example, organizational) are also included in the model. Due to the modular structure of DROPS, it is possible to integrate the essential elements of a security problem for specific business processes and their relationships into the model on an organization-specific basis. DROPS can be used to model current and/or target security requirements and an organization's security system [53].

Like approaches already familiar, DROPS is used to consider and analyze existing system components and organizational structures.

6.1.4 Tropos

Tropos is a software development methodology using the flexibility of Agent Oriented Programming (AOP). Tropos is based on two novel features: Firstly, in all phases of software development, it uses the notion of an agent and all related mental notions (such as goals and plans). These phases range from early analysis to actual implementation. Secondly, Tropos focuses on the initial phase, in which requirements are analyzed, so it leads to a deeper understanding of the environment in which the software is to be used and of the interactions between the software and human agents [54]. The five main development phases of the Tropos methodology are early requirements, late requirements, architectural design, detailed design, and implementation [54]. The Secure Tropos methodology is an extension of Tropos, to include the property of security. It supports security modeling and risk management [55].

The Tropos Method is used in the development and implementation of a system or software.

6.1.5 ISSRM Reference Model

The ISSRM activities are derived from the general risk management process. This process is divided into six steps. The first step defines the context of the organization and identity of its assets and then defines the security aims (confidentiality, integrity and/or availability). The next step is risk assessment to identify the risks harming assets and threatening security aims and is followed by decisions on how to treat the risks. This includes risk avoidance, risk reduction, risk transfer, and risk retention. Based on this analysis, the security requirements on the information systems are determined, leading to a reduction in the risks defined. As a final step, the requirements are instantiated into security controls. The ISSRM Reference Model is iterative, and new risks can be identified with each new run of the process [55].

The ISSRM Reference Model follows the principle of the risk-management process and is used with existing information systems.

6.1.6 Security and Risk Assessment in Cyber-Physical Systems

There are several approaches in academia to the topic of security and risk assessment in CPS. In [56], a methodology for assessing the security of a CPS is presented. The presented methodology automatically generates attack trees based on the system's architecture. Technical as well as non-technical feedback can be derived from the attack trees. The 4S framework [57] presents a model for security assessment of medical CPS. 4S stands for Step-by-Step, Systematic, Score Based, Security Pivotal Assessment & Benchmarking framework. It incorporates elements of model-driven security engineering principles and can be used to formulate benchmarking process to perform design-time security assessment. In "Risk Assessment Method for Cyber Security of Cyber Physical Systems" [58], a quantitative hierarchized assessment model is presented for assessing cyber-security risk of CPS. The model consists of attack severity, attack success probability, and attack consequences, and can be used to assess the risk caused by an ongoing attack at the host and system levels. A system with specific evaluation indicators for information security is presented in [59]. This is based on the criterion of system stability and the homeostatic approach. In [60], a security-oriented stochastic risk management method is presented. This method computes cyber-physical security indices to measure the security level of the underlying cyber-physical environment. In [61], an approach for modeling and quantitative assessment of CPS security is presented, which is based on cyber attack analysis.

6.1.7 Summary

The state of the art has shown that there are two approaches to security assessment that are also used in practice. On the one hand, these means security modeling, for example, according to BSI, ISO standards or the principle of security by design, and on the other hand, security modeling based on attack vectors. In both approaches, the focus lies on the requirement criterion of data security and the analysis takes place at system level. The existing process models are limited to the analysis of information systems in companies or are models for software development from the point of view of security. This security assessment focuses on the requirement criterion of data security or security in general. Data security is evaluated using the currently valid trust model. Existing procedures for security and risk assessment in CPS are related to the aspect of technical security and partly result from analyses of potential vulnerabilities and attacker modeling. In these publications on the subject of security and risk assessment in CPS, the topic of security assessment of CPS is dealt with, but only the requirement criterion of data security is considered here. No consideration and analysis (security modeling) of highly scalable, volatile systems is performed within this framework. An apt framework for security modeling must be developed for future systems endowed with the properties of being highly scalable and volatile. The aim is to develop a process-oriented framework for assessing the security of CPS.

In the security assessment model that should be developed, a framework is to be defined that takes into account not only the requirement criterion of data security, but also the other requirement criteria of CPS and a new trust model. The security assessment should not take place at system level, but should be process-based. This should enable a more detailed statement to be made about the security level of processes in CPS under the influence of the other requirement criteria and thus enable targeted and optimally suitable security measures to be selected.

6.2 Requirements Analysis for Security Assessment of Cyber-Physical Systems

The requirements for assessing the security of CPS may be described as follows. The data collectors and users can be humans and/or machines, processing or accessing data in real-time. In the case of Germany, there are about 41.5 million households[1] [62], so a smart grid must be highly scalable and volatile. There will be an elevated volume of data, varying in quantity, quality, and occurrence, creating the following requirements: data security, scalability, real-time, volatility, functional safety, connectivity, performance, computing time, and operating costs (compare Figure 6.1).

Data Security: Data security can be described as a requirement of CPS in security assessment. Here, data security combines confidentiality, availability, and integrity characteristics. In this context, confidentiality means that data and information are only made available to authorized users. Availability means that the data must be provided within a defined period of time and integrity means that the data is not falsified.

Scalability: The scalability requirement for CPS refers to the number of participants in a system. No distinction is made regarding whether participants are humans or machines. CPS are characteristically systems or networks with a large number of participants.

Real-time: Real-time specifies another requirement for the security assessment of CPS. The necessity of real-time differs depending on the application

[1] in 2019

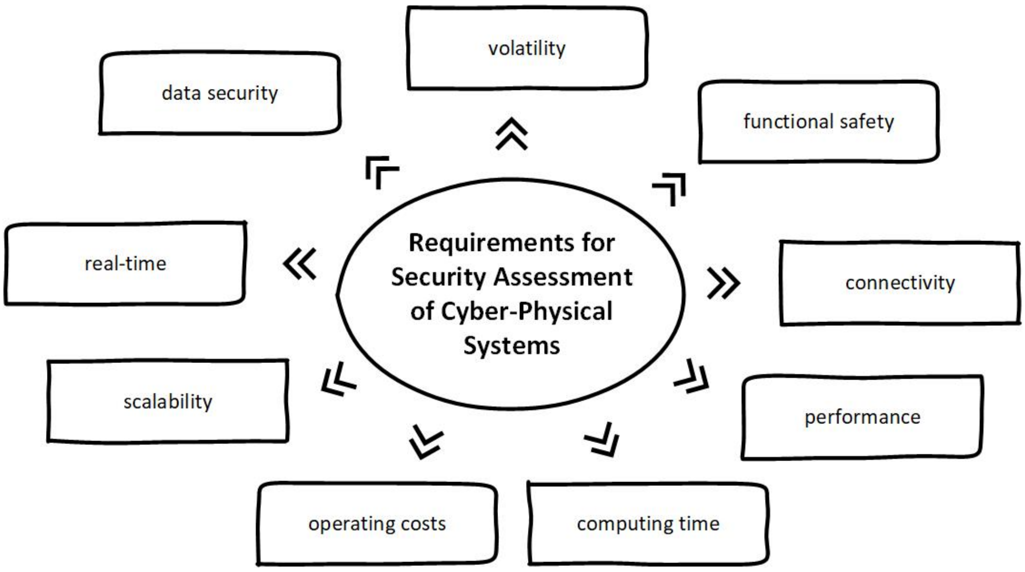

Figure 6.1: Requirements Analysis for Security Assessment of Cyber-Physical Systems

area. This is reflected in the different time specifications. Therefore, the real-time requirement must be re-examined for each application area.

Volatility: Volatility can be regarded as a further requirement criterion. In CPS, the "coming and going" of participants can be observed. In its most potent form, this requirement can be compared with ad hoc networks.

Functional Safety: Functional safety is a further requirement criterion in addition to classic data security. In the context of a CPS, it refers to the fail-safe nature of a system.

Connectivity: Connectivity concerns the requirement for systems to be observable from and in different areas as well as within application areas.

Performance: Performance refers to the efficiency of the CPS. In particular, hardware and memory are taken into account. Performance is to be considered in an overall context with scalability.

Computing time: Due to resource scarcity, another requirement is computing time. It must be considered in relation to the performance of the CPS.

Operating costs: Another requirement is the operating costs of the CPS. The measures to be implemented in a security assessment must be compatible with the added value and the operating costs.

In general, the requirements mentioned are not entirely new. Instead, they are a necessary enhancement of existing security assessment models. In fact, the known models only consider the aspect of data security with the characteristics of confidentiality, availability, and integrity. All the other requirements mentioned above have not yet been included in evaluation of classic security assessment.

Chapter 7

Model Development of Security Assessment for Cyber-Physical Systems

Due to the identified requirements for security assessments in CPS, only the development of the procedure model can be carried out. The requirements were derived from the state of the art in science, smart grid, and CPS. In this chapter, I define and present the model for security assessment for CPS. As an example, the security measure “authentication” is evaluated and integrated into the model. The model developed is then demonstrated by using a smart grid as an example.

7.1 Model Development of a Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

In the first developmental step, the focus is on the requirement of criteria data security (DS), scalability (SC), and real-time (RT). In the context of the security modeling of CPS, all three must be considered. The security assessment results from the process described by these criteria and is defined as follows:

$$\text{usecase}_{\text{process}} = (\text{DS, SC, RT}).$$

The result of the security assessment depends on the description of the process, and the framework for the security assessment (PROSA) is as follows. At first, the process, infrastructure, data, and information are analyzed. The security is then assessed in terms of data security, scalability, and real-time criteria. The last step is the automated mapping of the model based on the use case process and the assignment of security measures. Further requirements are performance, functional safety, volatility, connectivity, computing time, and operating costs, which will not be considered in the current work.

Figure 7.1 describes PROSA. The use case is divided into processes, and each process is assessed in terms of data security, scalability, and real-time criteria. A process description is derived, and security measures are automatically selected. In the following subsections, the specific attributes of the tuple are described in general terms.

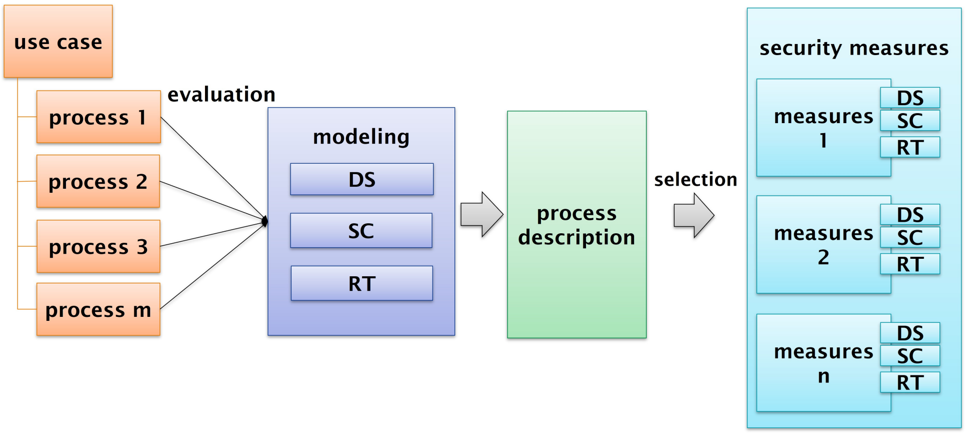

FIGURE 7.1: Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

7.1.1 Data Security Model

The 4-Level-Trust-Model for security-critical systems is a model for assessing the security of CPS. Classically, the data are put into the two categories *secure* and *insecure*. However, in the new 4-Level-Trust-Model for security-critical systems, the data are put into four categories [8]. The categorization depends on the requirements analysis for a CPS. The categories in the 4-Level-Trust-Model for security-critical systems are defined as follows.

1. Category: non-sensitive data
   - All data that have no personal reference or have been made anonymous.
   - There is no harm done, even to a person affected.
   - The level of security is low.
2. Category: highly sensitive data I
   - All data that, in combination with some data in categories 2 and 3, have a personal reference but do not have a personal reference themselves.
   - Harm is limited and manageable; harm done to a person affected is fairly easy to mend.
   - The level of security is minimal.
3. Category: highly sensitive data II
   - All data that, combined with some data in categories 2 and 3, have a personal reference but do not have a personal reference themselves.
   - The harm is felt to be significant by a person affected.
   - The security level is intermediate.

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

Table 7.1: Overview — Data Security

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

7.1.2 Scalability Model

Scalability describes the number of participants, here understood to be human users (human to machine interaction) and devices (machine to machine interaction). Scalability in this context is intended to show how many participants are involved in the process. This means, whether it is a process with a large number of participants or a process with very few participants. A participant is understood here as the classic human user as well as devices or systems. The model for scalability is represented by means of 4 categories. Category 1 always describes the minimum number of participants in a process. Category 4, on the other hand, describes the range of the number of participants where they can no longer be counted. Category 2 and 3 concern the average values. For the definition of these criteria, values related to the respective use case can also be used. Depending on the application, the limits must be adjusted. In the context of this thesis, the scalabiltiy model is divided into four categories using the smart grid application example (see Chapter 4.6).

In the smart grid application example, these thresholds are 2, 100, 10,000 and greater than 10,000, covering a classic household up to the entire system. The model for scalability is shown in Table 7.2 with the corresponding coding.

Table 7.2: Overview — Scalability

criteria: participant	coding
≤ 2	0
$3 \leq 100$	1
$101 \leq 10.000$	2
≥ 10.001	3

7.1.3 Real-Time Model

The characteristic of real-time requirement is derived from the principle “real-time systems are computer systems”. These are systems that must respond to events in the environment within precise time specifications. The correct behavior depends not only on the value of the calculation but also on the time required until the result is generated or the task is processed [63]. Real-time deadlines are classified as hard, firm or soft. “Hard” refers to when the consequences of non-compliance can be catastrophic. “Firm” refers to when the results achieved are no longer useful once the deadline expires, but the consequences of not meeting the deadline are not very severe. “Soft” refers to a deadline that is neither hard nor firm [64].

The real-time assessment model is also divided into 4 categories. Category 1 describes the requirements for hard real-time. Category 4 can be assigned to soft real-time requirements. Category 2 is a mixed category of the hard and fixed requirements. This involves processes that do not cause catastrophic damage in case of non-compliance, but damage with low impact. The third category contains processes that can be assigned to the criteria of the fixed real-time. The specific deadlines must be determined and defined depending on the application example.

Real-time is classified into four categories based on the smart grid use case (see Chapter 4.6). In the smart grid application example, these limit values are 1 sec, 1 min, 15 min and 1 h. The requirement criterion of real-time (1s) and the critical value for meter reading of 15 min are taken into account here. 1h means that no time conditions are imposed on the transmission of the respective information. 1 min describes the requirement for the transmission of data that is not in the real-time range and does not have to be transmitted in the 15 min requirement. Table 7.3 shows the modeling for real-time with the corresponding coding.

Table 7.3: Overview — Real-Time

criteria: time	**coding**
1 s	0
1 min	1
15 min	2
1 h	3

7.2 Selection of Security Measures

Based on PROSA, specific security measures can be chosen. The procedure “selection of security measure” is shown by using “authentication”, and measurements are analyzed and assessed in terms of the CPS requirement criteria. The criteria data security, scalability, and real-time will be used for the analysis. The last step of the framework presented consists of assigning the security measure of the corresponding security ratings.

7.2.1 Authentication Methods

This chapter analyzes the different authentication procedures and classifies them based on terms of data security, scalability, and real-time. The term authentication describes how an entity proves its identity to a communication partner. It is an identification used to transmit credentials. Authentication refers to the process of verifying or proving the authenticity of the information. It ensures that the specified identity matches the entity by comparing the selected attributes. If the identity is verified, the requesting entity may, for instance, access a resource. The term authorization describes the process of assigning rights to the requesting entity [65].

7.2.2 Definition of Assessment Criteria

Based on PROSA, it is possible to classify the processes. This enables suitable security measures to be chosen. For this, the security measures must firstly be ranked and evaluated. In literature, for example, the security measures are assessed in terms of operating costs or probabilities. The evaluation criteria correspond to the requirements derived from the requirements' analysis and consideration of CPS. The focus is on the following criteria.

- data security
- scalability
- real-time

The criteria are described below, along with the evaluation principles for analyzing authentication procedures.

Data Security
Data security focuses on the confidentiality and integrity of data. A key point is the security of the data, particularly personal data and data worth protecting. The criteria for the evaluation are taken from TR-03107 [66].

- low
  - the procedure must prevent attacks with low damage potential [66]
- intermediate
  - the procedure must prevent attacks with moderate damage potential [66]
- high
  - the procedure must prevent attacks with high damage potential [66]

Table 7.4: Overview — Evaluation Criteria Data Security

coding	data security
0	low
1	intermediate
2	high

Scalability

For the evaluation of scalability, the number of possible authentication operations at the same time is considered. The classification of levels of authentication determines the scalability into high, intermediate, and low. The level "high" means the authentication solution can cope with a growing number of subscribers; the level "intermediate" is partially scalable; and the level "low" is negligibly scalable.

Table 7.5: Overview — Evaluation Criteria Scalability

coding	scalability
0	low
1	intermediate
2	high

Real-time

Real-time is considered in the context of authentication measures. Here, the time factor is thought to affect the success of authentication. In other words, authentication is possible within a defined period, but if it is not, the effects on the user are considered. Furthermore, it is assumed that there is no need for a real-time requirement for specific use cases. In the following, the real-time requirement is divided into "hard", "soft", and "none", based on the explanation and defined for the application area of authentication in highly scalable, volatile systems.

- Soft real-time requirement
  - Violating the real-time requirement is tolerable [67].
  - Violating the real-time requirement slightly increases the cost [67].
- Hard real-time requirement
  - Violating the real-time requirement is catastrophic and intolerable [67].
  - Costs due to violating the real-time requirement increase massively [67].
- No real-time requirement
  - The precondition for a real-time requirement is not fulfilled.

  - With no real-time requirement, the period of the response is irrelevant.

TABLE 7.6: Overview — Evaluation Criteria Real-Time

coding	**real-time**
0	hard
1	soft
2	none

7.3 Evaluation of Authentication Methods

In this section, the following procedures are analyzed and evaluated with the criteria given (cf. Table 7.7).

- password
- public-key-cryptography
- one-time-password
- multi-factor authentication
- biometric authentication
- digital identity

TABLE 7.7: Overview — Evaluation Criteria

coding	**data security**	**scalability**	**real-time**
0	low	low	hard
1	intermediate	intermediate	soft
2	high	high	none

The procedure for analysis and evaluation is as follows:

- a short description of the method
- an assessment of the method
- an interpretation of the results

The “optimal” condition is taken to be the framework condition for the authentication questions, as well as for the mapping through a secure transmission path (communication path).

7.3.1 Password

Short Description of the Method

Authentication by the password method (username and password) can be described as follows: A user authenticates himself by proving knowledge of a secret shared with the system [14]. The password is a secret with which the password's owner can confirm his identity, but sharing a secret may lessen the security, so passwords are always stored with hash values [68].

Assessment of the Method

- Data security
  - Low (0)
  - Statement: Only the "low" security level can be achieved. The evaluation and the argumentation are taken from TR-03107 (compare [66]). The security of a password depends significantly on the choice of the "word" (all known phenomena, short passwords, words, or series of numbers). Furthermore, the security of a password depends on keeping it secret (not writing it down or being influenced by social engineering [66]).
- Scalability
  - High (2)
  - Statement: Only the scalability requirement "high" can be achieved. The scalability depends on the length of a password, which also influences security. To ensure a high level, a very secure password with at least eight characters according to the known password rules is assumed. Another criterion for scalability is the administration and secure storage of a password. This point also influences security.
- Real-time
  - Soft (1)
  - Statement: Only the real-time requirement "soft" can be achieved. The real-time requirement is influenced by various factors (for example, the management of a password). Besides these factors, security and scalability play a role, which impacts real-time.

Interpretation of the Results

For the evaluation of the password procedure, the result is as follows: 0,2,1. The requirement for a high level of security has an indirect impact on scalability, and the real-time requirement and scalability have an indirect effect on real-time requirements. The encryption and decryption of passwords — depending on the strength of the encryption algorithm — affects scalability and real-time. The stronger the algorithm, the weaker the scalability and real-time, but the security of the passwords is increased.

7.3.2 Public-Key-Infrastructure

Short Description of the Method

PKI refers to the components required for the infrastructure to generate and manage certificates. The infrastructure consists of the certification authority (CA) and the registration authority (RA) combined in a trust center. The rules for issuing and managing credentials are set out in the Certificate Policy and the Certification Practice Statement [14]. This requires a very high level of personnel and organizational effort.

Assessment of the Method

- Data security
  - High (2)
  - Statement: The confidence level "high" can be achieved. Attacks with the potential "high" are prevented. PKI is described as solid authentication [69]. This has been demonstrated by various scientific publications (for example [70, 14, 71]) and its use in highly critical areas.
- Scalability (1)
  - Intermediate
  - Statement: Scalability is rated as "intermediate". The scalability of the system is partially given. It is influenced by the management of the certificate and the choice of the encryption algorithm (keyword: overhead).
- Real-time (1)
  - Soft (1)
  - Statement: The real-time requirement is classified as "soft". By using the method, it must be possible to cope with violations of the real-time requirements. Real-time cannot be guaranteed due to the effort involved in checking and managing certificates. The time that the encryption takes for de- and encoding, as well as the exchange of the keys via the PKI at the beginning, must also be taken into account in this context.

Interpretation of the Results

For the evaluation of the PKI, the result is as follows: 2,1,1.
If a "high" level of security is achieved, there has to be a trade-off in scalability and real-time requirements. The level of security is influenced, for instance, by the management of the certificates and the key length or the method chosen for encryption.

7.3.3 One-Time-Password

Short Description of the Method
With the One-Time-Password method, the password is used only once for authentication [14]. A new password is generated for the user for each identification or authentication and is valid for only one use. Today, passwords are usually generated dynamically. A special algorithm is used that comes as close as possible to real chance when generating the password, so the next password cannot be guessed by finding a pattern [72].

Assessment of the Method

- Data security
  - Intermediate (1)
  - Statement: The confidence level "intermediate" can be achieved (cf. [66]). Attacks with the potential "moderate" are prevented. "High" can be achieved only if the TAN procedure is used. Here, essential data must be used to generate the TAN [66].
- Scalability
  - Intermediate (1)
  - Statement: Scalability is rated as "intermediate". The system scales partially. The scalability is affected by the generation of One-Time-Passwords and their secure distribution.
- Real-time
  - Soft (1)
  - Statement: The real-time requirement is classified as "soft". By using the method, it must be possible to cope with violations of the real-time requirements. Due to the effort to create the one-time passwords and the matching under the prerequisite "data security" medium, sacrifices in the real-time requirements must be accepted. The distribution/transmission of one-time passwords also affects the real-time request.

Interpretation of the Results
For the evaluation of the One-Time-Password, the result is as follows: 1,1,1. The scalability and real-time requirement depend on the creation and transmission of the One-Time-Password, which also influences the evaluation. The evaluation regarding data security has been taken from TR-03107-1.

7.3.4 Multi-Factor Authentication

Short Description of the Method
Various kinds of authentication factors can be used and combined in multifactor authentication. This exploits the advantages of the individual processes

and increases security. For example, a combination of knowledge and possession results in a two-factor authentication, which can be described as a strong personal connection through individual knowledge. It is essential with two-factor authentication that the two factors are different [73].

Assessment of the Method

- Data security
  - High (2)
  - Statement: The confidence level "high" can be achieved. Attacks with the potential "high" are prevented. The two factors chosen must be different, and at least one must already be rated as being at least "medium".
- Scalability
  - Low (0)
  - Statement: The scalability requirement is classified as low. The system scales only to a limited extent. Authentication requires not only one secret but multiple secrets for multi-factor authentication. The transfer, matching, etc., have an impact on scalability as well as on the choice of procedures in general.
- Real-time
  - Soft (1)
  - Statement: The real-time requirement is classified as "soft". By using this method, it must be possible to cope with violations of the real-time requirements. By using at least two factors, real-time authentication can no longer be guaranteed since authentication takes place in at least two steps.

Interpretation of the Results
For the evaluation of the Multi-factor Authentication, the result is as follows: 2,0,1.
The selection of the two procedures can influence data security. The use of at least two of them influences the scalability and real-time requirement.

7.3.5 Biometric Authentication

Short Description of the Method
Methods for biometric authentication can be divided into two classes. A distinction is made between methods based on the physiological, static features of a person (for example, iris, retina) and methods based on behavioral, dynamic (for example, typing behavior, voice) features. The requirements for using a biometric feature are that it should be

- universal

- unique
- durable
- quantitative
- performance (if dynamic)
- acceptable
- cannot be faked

The establishment of biometric authentication in the market has stalled due to the high costs of the equipment needed [14].

Assessment of the Method

- Data security
  - High (2)
  - Statement: The confidence level "high" can be achieved. Attacks with the potential "high" are prevented.
- Scalability
  - Intermediate (1)
  - Statement: The scalability is rated as "intermediate". The system scales partially.
- Real-time
  - Soft (1)
  - Statement: The real-time requirement is classified as "soft". By using the method, it must be possible to cope with violations of the real-time requirements.

Interpretation of the Results

For the evaluation of Biometric authentication, the result is as follows: 2,1,1. Biometric authentication is classified as a procedure with the security level "high". Real-time and scalability are influenced by the secure storage of the feature and the matching of the secret.

7.3.6 Digital Identity — Smart Card

Short Description of the Method

Digitalization is making digital identities for people and devices increasingly important [14]. The smart card, for example, can be assessed here. In practice, possession-based authentication techniques are mostly implemented with smart cards. The smart card now in use is a plastic card that comes in various forms. There are pure memory cards, such as telephone cards. There are also intelligent memory cards that have an additional security logic, which is usually used for PIN storage and verification. If these cards are also equipped with their own microprocessor and programmable memory, they are referred to as smart cards. These are used today primarily as a security tool, especially for authentication. Smart cards are used in various industries, for example as money cards or Visa cash cards in the banking sector, as campus and company cards or as SIM cards in cell phones, as health cards or as the digital ID card [14].

Assessment of the Method

- Data security
  - High (2)
  - Statement: The confidence level "high" can be achieved. Attacks with the potential "high" are prevented.
- Scalability
  - Intermediate (1)
  - Statement: The scalability is rated as "intermediate". The system scales partially.
- Real-time
  - Soft (1)
  - Statement: The real-time requirement is classified as "soft". By using the method, it must be possible to cope with violations of the real-time requirements.

Interpretation of the Results
For the evaluation of the smart card, the result is as follows: 2,1,1.
Digital identification is classified as a procedure with the security level "high". Real-time and scalability are influenced by secure storage of the feature and matching of the secret. A Digital Identity is like a biometric characteristic in terms of classification and evaluation.

7.3.7 Summary

Table 7.8 shows an overview of the evaluation of the selected procedures. The assessment concerning data security was carried out in relation to known criteria; the methods were reclassified in terms of scalability and real-time requirements. The criterion used was the possible mapping of scalability and real-time requirements.

Table 7.8: Overview — Assessment of the Authentication Methods

method	DS	SC	RT
Password	0	2	1
PKI	2	1	1
One-Time-Password	1	1	1
Multi-Factor Authentication	2	0	1
Biometric Authentication	2	1	1
Digital Identity	2	1	1

7.4 Mapping Between Security Assessment and Security Measures

In this chapter, the security assessment criteria are assigned to the corresponding security measures. The assignment of the security assessment to the security measures is necessary as different metrics were used for the assessment. Thus, no direct assignment of the security assessment to the corresponding security measure can take place (see column “security assessment” and column “measure assessment” of Table 7.9). The assignment is necessary for the selection of the security measure after the security assessment. It was decided that the data security criterion would be weighted twice to become the main one for assignment. Another assignment had to be made with regard to the assessment of security measures. It was not possible to assign a specific security measure to every possible combination of security measure ratings. (see “mapping” column of Table 7.9). This procedure must be carried out for each future security measure.

The idea of Table 7.9 is to assign the appropriate security measure to the respective security assessment, with the aim of obtaining a mapping for the selection of security measures. It is not possible to assign corresponding security measures for every combination that results from the evaluation scheme for measures (measure assessment). Thus, there are possible combinations of measure evaluations that do not match any security measure evaluation result. With the result from the table, a corresponding security measure can be selected. In the first step, a comparison of security assessment and security measures was made. A one-to-one mapping is not possible due to the different metrics of security assessment and security measure. As already described in the previous paragraph, the focus is on the criterion of data security, which is regarded as the leading criterion. This means data security is given double weighting compared to the other criteria of real-time and scalability. The assignment of the security measure to the security evaluation was carried out according to the schemes that first of all an assignment of evaluation possibilities of the security measures was made to each possibility of the security evaluation. For the security measure evaluation possibility, where no match was possible, the value was reduced by 1. The leading criterion was data security. This means that the assignment was based on data security. Looking at entry 16 in Table 7.9, the security assessment score (0,3,3) is the corresponding assignment of security measures (0,2,2). As a second step, a mapping of the table was performed with the aim of selecting appropriate security measures based on these values. The mapping was done using the security measures authentication (see Chapter 7.3). Data security was also the leading criterion in the mapping process. This means that data security was adopted. The corresponding ratings from Chapter 7.3 were inserted and adjusted on the basis of these scalability and real-time. The mapping table must be created for each additional type of security measure.

The procedure for selecting suitable security measures based on the security assessment can be described as follows. If a security assessment is performed using PROSA with (1,2,0), the entry in line 25 of Table 7.9 in the "mapping" column is compatible with the corresponding coding for the selection of security measures.

Table 7.9: Mapping Table: Security Assessment and Measures Assessment

	security assessment			**measure assessment**			**mapping**		
#	**DS**	**SC**	**RT**	**DS**	**SC**	**RT**	**DS**	**SC**	**RT**
1	0	0	0	0	0	0	0	2	1
2	0	0	1	0	0	1	0	2	1
3	0	0	2	0	0	1	0	2	1
4	0	0	3	0	0	2	0	2	1
5	0	1	0	0	1	0	0	2	1
6	0	1	1	0	1	1	0	2	1
7	0	1	2	0	1	1	0	2	1
8	0	1	3	0	1	2	0	2	1
9	0	2	0	0	1	0	0	2	1
10	0	2	1	0	1	1	0	2	1
11	0	2	2	0	1	1	0	2	1
12	0	2	3	0	1	2	0	2	1
13	0	3	0	0	2	0	0	2	1
14	0	3	1	0	2	1	0	2	1
15	0	3	2	0	2	1	0	2	1
16	0	3	3	0	2	2	0	2	1
17	1	0	0	1	0	0	1	1	1
18	1	0	1	1	0	1	1	1	1
19	1	0	2	1	0	1	1	1	1
20	1	0	3	1	0	2	1	1	1
21	1	1	0	1	1	0	1	1	1
22	1	1	1	1	1	1	1	1	1
23	1	1	2	1	1	1	1	1	1
24	1	1	3	1	1	2	1	1	1
25	1	2	0	1	1	0	1	1	1
26	1	2	1	1	1	1	1	1	1
27	1	2	2	1	1	1	1	1	1
28	1	2	3	1	1	2	1	1	1

29	1	3	0	1	2	0	1	1	1
30	1	3	1	1	2	1	1	1	1
31	1	3	2	1	2	1	1	1	1
32	1	3	3	1	2	2	1	1	1
33	2	0	0	2	0	0	2	1	1
34	2	0	1	2	0	1	2	1	1
35	2	0	2	2	0	1	2	1	1
36	2	0	3	2	0	2	2	1	1
37	2	1	0	2	1	0	2	1	1
38	2	1	1	2	1	1	2	1	1
39	2	1	2	2	1	1	2	1	1
40	2	1	3	2	1	2	2	1	1
41	2	2	0	2	1	0	2	1	1
42	2	2	1	2	1	1	2	1	1
43	2	2	2	2	1	1	2	1	1
44	2	2	3	2	1	2	2	1	1
45	2	3	0	2	2	0	2	1	1
46	2	3	1	2	2	1	2	1	1
47	2	3	2	2	2	1	2	1	1
48	2	3	3	2	2	2	2	1	1
49	3	0	0	2	0	0	2	0	1
50	3	0	1	2	0	1	2	0	1
51	3	0	2	2	0	1	2	0	1
52	3	0	3	2	0	2	2	0	1
53	3	1	0	2	1	0	2	1	1
54	3	1	1	2	1	1	2	1	1
55	3	1	2	2	1	1	2	1	1
56	3	1	3	2	1	2	2	1	1
57	3	2	0	2	1	0	2	1	1
58	3	2	1	2	1	1	2	1	1
59	3	2	2	2	1	1	2	1	1
60	3	2	3	2	1	2	2	1	1
61	3	3	0	2	2	0	2	1	1
62	3	3	1	2	2	1	2	1	1
63	3	3	2	2	2	1	2	1	1
64	3	3	3	2	2	2	2	1	1

7.5 Case Study Smart Grid

In this chapter, PROSA is tested in practice within the scope of an empirical study. The process model exemplified above is again presented and tested using the "smart grid" application. In particular, the following examples of application are tested:

- smart metering
- feed-in and load management

- SEGAL (value-added service)

The application examples were described in Chapter 4.6. They are evaluated using the procedure described in Chapter 7.1. In the first step, the method involves dividing the use case into processes. Then, the data, information and the participants are determined and evaluated using the evaluation scheme for each process. With the result from the security evaluation, the appropriate security measures can be selected using the mapping table.

7.5.1 Use Case: Smart Metering

The use case “smart metering” refers to the transmission of energy values (electricity consumption values). The electricity consumption values are transmitted every 15 minutes (compare Chapter 4.6.1) The “smart metering” use case is divided into the following sub-processes:

- process 1: register device
- process 2: delete device
- process 3.1: update (1 user)
- process 3.2: update (multiple users)
- process 4: read meter data

Below, each process is evaluated using the approach presented above.

7.5.1.1 Process 1: Register Device

Data and Information
The following data and information are generated or transmitted during process 1 “Register Device”. When registering a smart meter, the following data are generated: meter-ID, gateway-ID, backend-system smart grid, and customer data ID.

Participants
The following participants are involved in the generation and transmission of the data: smart meter, smart meter gateway, SMGW admin, energy supplier, and backend-system smart grid.

Data Security
The data obtained are now evaluated regarding data security based on the defined criteria. No personal data are processed in process 1. It is data of the 3rd category that is processed. If one piece of information is combined with another, it is possible to draw conclusions about the user.

TABLE 7.10: Data Security — Process 1: Register Device

category	**description**	**security level**	**coding**
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability
The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability, at least six participants can be assumed.

TABLE 7.11: Scalability — Process 1: Register Device

participant	**coding**
$3 \leq 100$	1

The scalability is rated as 1.

Real-time
The process is now evaluated regard to the criteria of "real-time". For process 1, the device's initialization must take place within 15 min. No real-time requirement is given. The initialization must take no longer than 15 min.

TABLE 7.12: Real-Time — Process 1: Register Device

time	**coding**
15 min	2

The real-time is rated as 2.

Summary
The analysis yields the following definition for the role of "smart metering":
$\text{Smart\_Metering}_{\text{device\_register}} = (2,1,2)$.

Selection: security measure
The mapping table refers to a security measure with the rating (2,1,1).

7.5.1.2 Process 2: Delete Device

Data and Information
During process 2: Delete Device, the following data is generated or transmitted. When deleting a smart meter, the following data is generated: meter-ID, gateway-ID, backend-system smart grid and customer data ID.

Participants
Process 2 involves the following: smart meter, smart meter gateway, SMGW admin, energy supplier, backend-system smart grid.

Data Security

The data obtained are now evaluated concerning data security on the basis of the defined criteria. No personal data are processed in process 2. Only data of the 3rd category that are processed. If one piece of information is combined with another, it is possible to draw conclusions about the user.

Table 7.13: Data Security — Process 2: Delete Device

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability, at least six participants can be assumed.

Table 7.14: Scalability — Process 2: Delete Device

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated regarding the criteria of "real-time". For process 2, the device must be deleted within 15 min. No real-time requirement is given, but data must be deleted within 15 min.

Table 7.15: Real-Time — Process 2: Delete Device

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of "smart metering": $\text{Smart\_Metering}_{\text{device\_delete}} = (2,1,2)$.

Selection: security measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.1.3 Process 3.1: Update (Single User)

Data and Information

In process 3.1, update, the following data are generated or transmitted: meter-ID, gateway-ID, backend-system smart grid, customer data ID, update information.

Participants

The following participants are involved in process 3.1: smart meter, smart meter gateway, SMGW admin, energy supplier and backend-system smart grid.

Data Security

The data obtained are now evaluated concerning data security based on the defined criteria. No personal data are processed in process 3.1. User-specific data but no data with a direct personal reference should be transferred. Relationships between data transferred allow conclusions to be drawn about a user.

TABLE 7.16: Data Security — Process 3.1 Update (Single User)

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability, at least six participants can be assumed.

TABLE 7.17: Scalability — Process 3.1 Update (Single User)

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated regarding the criteria of "real-time". For process 3.1, the update must take place within 15 min. No real-time requirement is given, but data must be transferred within 15 min.

TABLE 7.18: Real-Time — Process 3.1 Update (Single User)

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of "smart metering":
$\text{Smart\_Metering}_{\text{update\_1\_User}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.1.4 Process 3.2: Update (Multiple User)

Data and Information

In process 3.2, update, the following data are generated or transmitted: meter-ID, gateway-ID, backend-system smart grid, customer data ID, update information.

Participants

The following participants are involved in process 3.2: all smart meters of the system, smart meter gateways of the system, SMGW admin, energy supplier, backend-system smart grid.

Data Security

The data obtained are now evaluated concerning data security on the basis of the defined criteria. No personal data are processed in process 3.2. Process 3.2 describes a process of system updating. No personal but only system-related data are transferred, these allow conclusions be drawn about a person only if some data are put together.

Table 7.19: Data Security — Process 3.2: Update (Multiple User)

category	description	security level	coding
category 2	highly sensitive data I	minimal	1

The data are assigned to the 2nd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". System updates, in this process, generally affect all users, so the whole system or all participants must be considered.

Table 7.20: Scalability — Process 3.2: Update (Multiple User)

participant	coding
>= 10.001	3

The scalability is rated as 3.

Real-time

The process is now evaluated with regard to the criteria of "real-time". For process 3, the update must take place within 15 minutes. No real-time requirement is given, but data must be transferred within 15 min.

Table 7.21: Real-Time — Process 3.2: Update (Multiple User)

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “smart metering”: $\text{Smart\_Metering}_{\text{update\_multiple\_User}} = (1,3,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (1,2,1).

7.5.1.5 Process 4: Read Meter Data

Data and Information

In process 4, read meter data, the following data are generated or transmitted: meter-ID, gateway-ID, backend-system smart grid, customer data ID, current consumption value.

Participants

The following participants are involved in process 4: Bei dem Prozess 4 sind folgenden Teilnehmer beteiligt: smart meter, smart meter gateway, SMGW admin, energy supplier and backend-system smart grid.

Data Security

The data obtained are now evaluated with regard to data security based on the defined criteria. No personal data are transferred during the “Read Meter Data” process. The gateway ID, customer ID, meter ID, and the current consumption value are thereby shared. The data allows conclusions to be drawn about a person only if at least two are put together.

Table 7.22: Data Security — Process 4: Read Meter Data

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for “scalability”. Considering the scalability, at least six participants can be assumed:

Table 7.23: Scalability — Process 4: Read Meter Data

participant	coding
$3 \leq 100$	1

The scalability is rated as 2.

Real-time

The process is now evaluated with regard to the criteria of “real-time”. For process 4, the update must take place within 15 min. No real-time request is available, but data must be transferred within 15 min.

Table 7.24: Real-Time — Process 4: Read Meter Data

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “smart metering”: $\text{Smart\_Metering}_{\text{read\_meter\_data}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.1.6 Summary: Use Case Smart Metering

The smart metering use case was evaluated based on the identified processes. The processes were assessed using the procedural model developed for security evaluation. Table 7.25 summarizes the results.

Table 7.25: Summary — Use Case Smart Metering

process	security assessment	security measure
process 1	2,1,2	2,1,1
process 2	2,1,2	2,1,1
process 3.1	2,1,2	2,1,1
process 3.2	1,3,2	1,2,1
process 4	2,1,2	2,1,1

Processes 1, 2, 3.1, and 4 are the same in the security assessment and describe the basic processes and the update of a single user. Process 3.2 differs mainly in the number of participants. In the case of system updates, all participants are affected. Figure 7.2 summarizes the results of the security assessment.

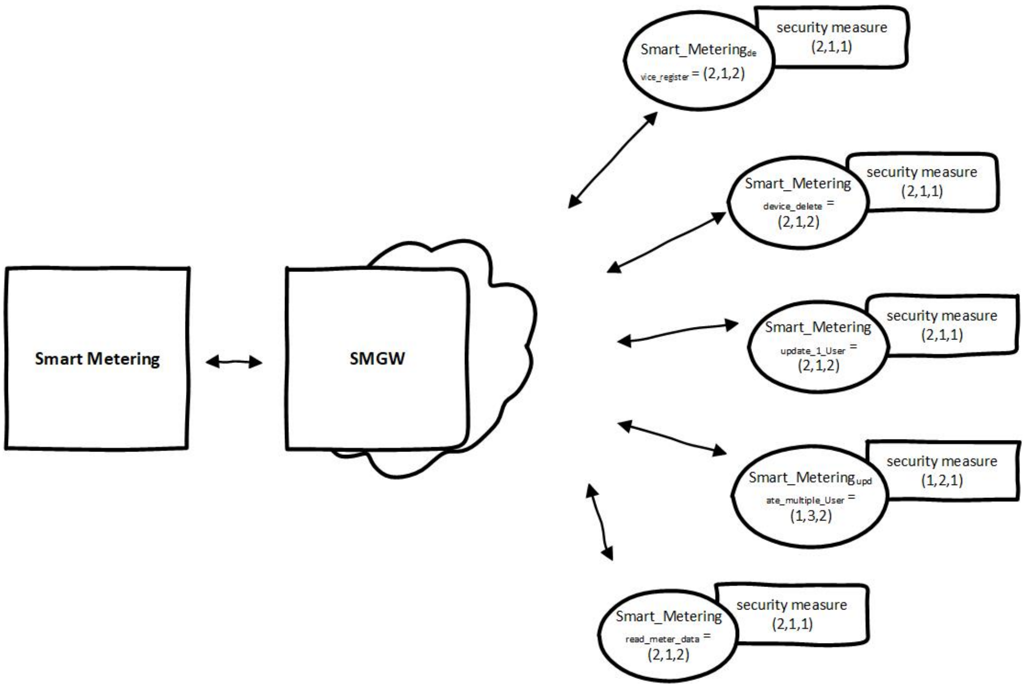
Smart Metering
SMGW
Smart_Metering device_register = (2,1,2)
security measure (2,1,1)
Smart_Metering device_delete = (2,1,2)
security measure (2,1,1)
Smart_Metering update_1_User = (2,1,2)
security measure (2,1,1)
Smart_Metering update_multiple_User = (1,3,2)
security measure (1,2,1)
Smart_Metering read_meter_data = (2,1,2)
security measure (2,1,1)

FIGURE 7.2: Security Assessment Use Case Smart Metering

7.5.2 Use Case: Feed-In and Load-Management

The use case “feed-in and load management” refers to the management of energy feed-in on the one hand and the distribution of loads with the addition and removal of generators on the other hand (cf. Chapter 4.6.2). The use case “feed-in and load management” is divided into the following sub-processes:

- process 1: register device (switching box)
- process 2: delete device (switching box)
- process 3.1: update (single user)
- process 3.2: update (multiple users)
- process 4: register system
- process 5: delete system
- process 6: read values
- process 7: carry out a measure

Below, each process is evaluated based on the approach presented.

7.5.2.1 Process 1: Register Device (Switching Box)

Data and Information

Process 1, register device (switching box), generates and transmits the following data and information: switching box ID, meter-ID, gateway-ID, backend-system smart grid, customer data ID.

Participants

The following participants are involved in process 1: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier and backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 1. Only data of the 3rd category that are processed. If one piece of information is combined with another, it is possible to draw conclusions about the user.

Table 7.26: Data Security — Register Device (Switching Box)

category	**description**	**security level**	**coding**
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for “scalability”. Considering the scalability, at least seven participants can be assumed.

Table 7.27: Scalability — Register Device (Switching Box)

participant	**coding**
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of “real-time”. For process 1, the device’s initialization must take place within 15 min. No real-time requirement is given. The initialization must take no longer than 15 min.

Table 7.28: Real-Time — Register Device (Switching Box)

time	**coding**
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “feed-in and load management”: $\text{Feed-in\_Load\_Management}_{\text{device\_register}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.2 Process 2: Delete Device

Data and Information

In process 2, delete device, the following data and information are generated and transmitted: switching box ID, meter-ID, gateway-ID, backend-system smart grid, customer data ID.

Participants

The following participants are involved in the generation and transmission of the data: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 1. Only data of the 3rd category are processed. If one piece of information is combined with another, it is possible to draw conclusions about the user.

Table 7.29: Data Security — Delete Device

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability, at least seven participants can be assumed.

Table 7.30: Scalability — Delete Device

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of "real-time". For process 1, the initialization of the device must take place within 15 min. No real-time requirement is given. The initialization should take no longer than 15 min.

Table 7.31: Real-Time — Delete Device

time	coding
15 min	2

The real-time is rated as 2.

Summary
The analysis yields the following definition for the role of "feed-in and load management": Feed-in_Load_Management$_{\text{device\_delete}}$ = (2,1,2).

Selection — Security Measure
The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.3 Process 3.1: Update (Single User)

Data and Information
In process 3.1, update, the following data are generated or transmitted: meter-ID, switching box-ID, gateway-ID, backend-system smart grid, customer data ID, update information.

Participants
The following participants are involved in process 3.1: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier, backend-system.

Data Security
The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 3.1. User-specific data may be transferred as part of this process, but not data with a direct personal reference. The data in combination can enable conclusions about a user.

Table 7.32: Data Security — Process 3.1: Update (Single User)

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability
The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability, at least seven participants can be assumed.

Table 7.33: Scalability — Process 3.1: Update (Single User)

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time
The process is now evaluated regarding the criteria of "real-time". For process 3.1, the update must take place within 15 min. No real-time requirement is given. The initialization should take no longer than 15 min.

TABLE 7.34: Real-Time — Process 3.1: Update (Single User)

time	coding
15 min	2

The real-time are is rated as 2.

Summary

The analysis yields the following definition for the role of "feed-in and load management": Feed-in_Load_Management$_{\text{update\_1User}}$ = (2,1,2).

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.4 Process 3.2: Update (Multiple User)

Data and Information

In process 3.2, update, the following data are generated or transmitted: meter-ID, switching box-ID, gateway-ID, backend-system smart grid, customer data ID, update information.

Participants

The following participants are involved in process 3.2: all smart meters of the system, all switching boxes of the system, all smart meter gateways of the system, SMGW admin, energy supplier, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 3.2. Process 3.2 describes a process of system updating. No personal but only system-related data are transferred that allow conclusions be drawn about a person only if some data are put together. Only system settings are made as part of this process.

TABLE 7.35: Data Security — Process 3.2: Update (Multiple User)

category	description	security level	coding
category 2	highly sensitive data I	minimal	1

The data are assigned to the 2nd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". System updates in this process generally affect all users, so the whole system or all participants must be considered.

Table 7.36: Scalability — Process 3.2: Update (Multiple User)

participant	**coding**
>= 10.001	3

The scalability is rated as 3.

Real-time

The process is now is evaluated with regard to the criteria of "real-time". For process 3, the update must take place within 15 minutes. No real-time requirement is given. The initialization should take no longer than 15 min.

Table 7.37: Real-Time — Process 3.2: Update (Multiple User)

time	**coding**
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of "feed-in and load management": Feed-in_Load_Management$_{\text{update\_multiple\_user}}$ = (1,3,2).

Selection — Security Measure

The mapping table refers to a security measure with the rating (1,2,1).

7.5.2.5 Process 4: Register System

Data and Information

In process 4, register system, the following data are generated or transmitted: meter-ID, switching box-ID, gateway-ID, backend-system smart grid, customer data ID.

Participants

Process 4 involves the following participants: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 4. It processes data of the 3rd category. If one piece of information is combined with another, it is possible to draw conclusions about the user. Customer-specific data are transferred as part of this sub-process.

Table 7.38: Data Security — Process 4: Register System

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability, at least seven participants can be assumed.

Table 7.39: Scalability — Process 4: Register System

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of "real-time". For process 4, the registration of the system must take place within 15 min. No real-time requirement is given. The initialization should take less than 15 min.

Table 7.40: Real-Time — Process 4: Register System

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of "feed-in and load management": Feed-in_Load_Management$_{\text{register\_system}}$ = (2,1,2).

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.6 Process 5: Delete System

Data and Information

In process 5, delete system, the following data are generated or transmitted: meter-ID, switching box-ID, gateway-ID, backend-system smart grid, customer data ID.

Participants

The following participants are involved in process 5: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 5. It processes data of the 3rd category. If one piece of information is combined with another, it is possible to draw conclusions about the user. Customer-specific data are transferred as part of this sub-process.

Table 7.41: Data Security — Process 5: Delete System

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for “scalability”. Considering the scalability, at least seven participants can be assumed.

Table 7.42: Scalability — Process 5: Delete System

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of ”real-time“. For process 5, the system must be cleared within 15 minutes. No real-time requirement is given. The action should take less than 15 min.

Table 7.43: Real-Time — Process 5: Delete System

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of ”feed-in and load management“:
Feed-in_Load_Management$_{\text{delete\_system}}$ = (2,1,2).

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.7 Process 6: Read Values

Data and Information

In process 6, read values, the following data are generated or transmitted:

meter-ID, switching box-ID, gateway-ID, backend-system smart grid, customer data ID, current consumption values.

Participants

The following participants are involved in process 6: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 6. It processes data of the 3rd category. If one piece of information is combined with another, it is possible to draw conclusions about the user. Current consumption values are transferred as part of this sub-process.

Table 7.44: Data Security — Process 6: Read Values

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for ”scalability“. Considering the scalability, at least seven participants can be assumed.

Table 7.45: Scalability — Process 6: Read Values

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of “real-time”. For process 6, the transmission of the current values must take place within 15 min. No real-time requirement is given. The action should take less than 15 min.

Table 7.46: Real-Time — Process 6: Read Values

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “feed-in and load management”: $\text{Feed-in\_Load\_Management}_{\text{read\_values}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.8 Process 7: Carry Out Measure

Data and Information

In process 7, carry out measure, the following data are generated or transmitted: meter-ID, switching box-ID, gateway-ID, backend-system smart grid, customer data ID, measure.

Participants

Process 7 involves the following participants: smart meter, switching box, smart meter gateway, SMGW admin, energy supplier, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 7. It processes data of the 3rd category. If one piece of information is combined with another, it is possible to draw conclusions about the user. Customer-specific data are transferred as part of this sub-process.

Table 7.47: Data Security — Process 7: Carry Out Measure

category	**description**	**security level**	**coding**
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for “scalability”. Considering the scalability, at least seven participants can be assumed.

Table 7.48: Scalability — Process 7: Carry Out Measure

participant	**coding**
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of “real-time”. For process 7, the execution of the measure must take place within 15 min. No real-time requirement is given. The initialization should take less than 15 min.

TABLE 7.49: Real-Time — Process 7: Carry Out Measure

time	coding
15 min	2

The real-time is rated as 2.

Summary
The analysis yields the following definition for the role of "feed-in and load management": $\text{Feed-in\_Load\_Management}_{\text{carry\_out\_measure}} = (2,1,2)$.

Selection — Security Measure
The mapping table refers to a security measure with the rating (2,1,1).

7.5.2.9 Summary: Use Case Feed-In and Load Management

The feed-in and load management use case was evaluated based on the identified processes. The processes were evaluated using the developed process model for security assessment. Table 7.50 summarizes the results.

TABLE 7.50: Summary — Use Case Feed-In and Load Management

process	security assessment	security measure
process 1	2,1,2	2,1,1
process 2	2,1,2	2,1,1
process 3.1	2,1,2	2,1,1
process 3.2	1,3,2	1,2,1
process 4	2,1,2	2,1,1
process 5	2,1,2	2,1,1
process 6	2,1,2	2,1,1
process 7	2,1,2	2,1,1

Processes 1, 2, 3.1, 4, 5, and 6 are the same in the security assessment and describe the basic processes and the update of a single user. Process 3.2 differs mainly in the number of participants. In the case of system updates, all participants are affected. Figure 7.3 summarizes the results of the security assessment.

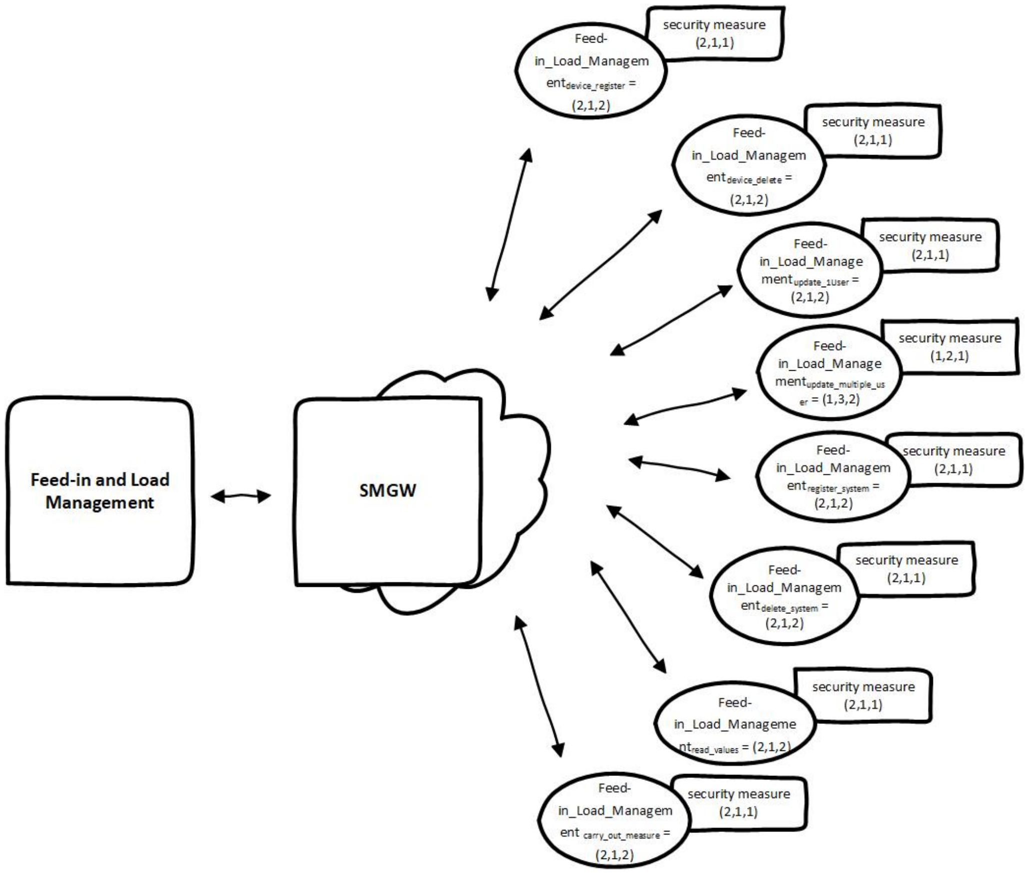
Feed-in and Load Management
SMGW
Feed-in_Load_Management$_{device\_register}$ = (2,1,2)
security measure (2,1,1)
Feed-in_Load_Management$_{device\_delete}$ = (2,1,2)
security measure (2,1,1)
Feed-in_Load_Management$_{update\_1User}$ = (2,1,2)
security measure (2,1,1)
Feed-in_Load_Management$_{update\_multiple\_user}$ = (1,3,2)
security measure (1,2,1)
Feed-in_Load_Management$_{register\_system}$ = (2,1,2)
security measure (2,1,1)
Feed-in_Load_Management$_{delete\_system}$ = (2,1,2)
security measure (2,1,1)
Feed-in_Load_Management$_{read\_values}$ = (2,1,2)
security measure (2,1,1)
Feed-in_Load_Management $_{carry\_out\_measure}$ = (2,1,2)
security measure (2,1,1)

FIGURE 7.3: Security Assessment Use Case Feed-In and Load Management

7.5.3 Use Case: Secure Gateway Service for Ambient Assisted Living

The SEGAL use case describes a value-added service for the smart grid infrastructure. In short, it transmits AAL data via the smart meter gateway to a remote control center (compare Chapter 4.6.3). The SEGAL use case is divided into the following sub-processes:

- process 1: register device
- process 2: delete device
- process 3.1: update (single user)
- process 3.2: update (multiple users)
- process 4: transmit data
- process 5: transmit emergency data
- process 6: transmit analyzed data

Below, each process is evaluated based on the approach presented.

7.5.3.1 Process 1: Register Device

Data and Information

In process 1, register device, the following data and information are generated and transmitted: device IT, customer data ID, hub-ID, SMGW ID.

Participants

The following participants generate and transmit the data: AAL-device, SMGW, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated concerning data security on the basis of the defined criteria. No personal data are processed in process 1. Only data of the 3rd category are processed. If one piece of information is combined with another, it is possible to draw conclusions about the user.

TABLE 7.51: Data Security — Process 1: Register Device

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability of the SEGAL service, a minimum of seven participants can be assumed. The backend-system is regarded as being one participant/device.

TABLE 7.52: Scalability — Process 1: Register Device

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of "real-time". For process 1, the registration of the device must take place within 15 min. No real-time requirement is given. The registration data must be transferred within 15 min.

TABLE 7.53: Real-Time — Process 1: Register Device

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of "SEGAL": $\text{SEGAL}_{\text{register\_device}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.3.2 Process 2: Delete Device

Data and Information

Process 2, delete device, generates and transmits the following data and information: device IT, customer data ID, hub-ID, SMGW ID.

Participants

The following participants are involved in generating and transmitting the data: AAL-device, SMGW, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated with regard to data security based on the defined criteria. No personal data are processed in process 2. Only data of the 3rd category are processed. If one piece of information is combined with another, it is possible to conclude the user.

Table 7.54: Data Security — Process 2: Delete Device

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability of the SEGAL service, a minimum of seven participants can be assumed. The backend-system is regarded as being one participant/device.

Table 7.55: Scalability — Process 2: Delete Device

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of "real-time". For process 1, the deletion of the device must take place within 15 min. No real-time requirement is given. The data must be transferred within 15 min.

Table 7.56: Real-Time — Process 2: Delete Device

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “SEGAL”: $\text{SEGAL}_{\text{delete\_device}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.3.3 Process 3.1: Update (Single User)

Data and Information

In process 3.1, update, the following data, and information are generated and transmitted: device ID, customer data ID, hub-ID, SMGW ID, update information.

Participants

The following participants are involved in process 3.1: AAL-device, SMGW, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated with regard to data security based on the defined criteria. No personal data are processed in process 3.1. In the “SEGAL” use case, AAL data are transmitted. These can also be medical data/information, such as the concentration of glucose in the blood, but may not be explicitly personal.

Table 7.57: Data Security — Process 3.1: Update (Single User)

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for “scalability”. Considering the scalability of the SEGAL service, a minimum of seven participants can be assumed. The backend-system is regarded as being one participant/device.

Table 7.58: Scalability — Process 3.1: Update (Single User)

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of “real-time”. For process 3.1, the update must take place within 15 min. No real-time requirement is given. The data must be transferred within 15 min.

Table 7.59: Real-Time — Process 3.1: Update (Single User)

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “SEGAL”: $\text{SEGAL}_{\text{update\_1User}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.3.4 Process 3.2: Update (Multiple User)

Data and Information

In process 3.2, update, the following data, and information are generated and transmitted: device IT, customer data ID, hub-ID, SMGW ID, update information.

Participants

The following participants are involved in process 3.2 of the data: all AAL-devices of the system, all SMGW of the system, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 3.2. Process 3.2 describes a process of system updating. During this sub-process, system data are transferred (system update).

Table 7.60: Data Security — Process 3.2: Update (Multiple User)

category	description	security level	coding
category 2	highly sensitive data I	minimal	1

The data are assigned to the 2nd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". System updates, as in this process, generally affect all users, so the whole system or all participants must be considered. The number of participants cannot be estimated since the ecosystem is viewed as a whole.

Table 7.61: Scalability — Process 3.2: Update (Multiple User)

participant	coding
>= 10.001	3

The scalability is rated as 3.

Real-time

The process is now evaluated with respect to the "real-time" criteria. No real-time requirement is given.

Table 7.62: Real-Time — Process 3.2: Update (Multiple User)

time	coding
1 h	3

The real-time is rated as 3.

Summary

The analysis yields the following definition for the role of "SEGAL":
$\text{SEGAL}_{\text{update\_multiple\_User}} = (1, 3, 3)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (1,2,2).

7.5.3.5 Process 4: Transmit Data

Data and Information

Process 4, transmit data, generates and transmits the following data and information: device IT, customer data ID, hub-ID, SMGW ID, medical data.

Participants

Process 4 involves the following participants: AAL-device, SMGW, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 4. It processes data of the 3rd category. If one piece of information is combined with another, it is possible to draw conclusions about the user. In the “SEGAL” use case, AAL data are transferred according to schemes. These can also be medical data/information, such as the concentration of glucose in the blood, but may not be explicitly personal.

Table 7.63: Data Security — Process 4: Transmit Data

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for “scalability”. Considering the scalability of the SEGAL service, a minimum of seven participants can be assumed. The backend system is regarded as being one participant/device.

Table 7.64: Scalability — Process 4: Transmit Data

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of “real-time”. For process 4, the values must be transmitted within 15 min. No real-time requirement is given. The measure should take no longer than 15 min.

Table 7.65: Real-Time — Process 4: Transmit Data

time	coding
15 min	2

The real-time is rated as 2.

Summary

The analysis yields the following definition for the role of “SEGAL”:
$\text{SEGAL}_{\text{transmit\_data}} = (2,1,2)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,1).

7.5.3.6 Process 5: Transmit Emergency Data

Data and Information

Process 5, transmit emergency data, generates and transmits the following data and information: device IT, customer data ID, hub-ID, SMGW ID, medical data, emergency data.

Participants

The following participants are involved in process 5: AAL-device, SMGW, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated concerning data security on the basis of the defined criteria. No personal data are processed in process 5. It processes data of the 3rd category. If one piece of information is combined with another, it is possible to draw conclusions about the user. In the "SEGAL" use case, AAL data are transmitted. AAL data can also be medical data/information, such as the glucose concentration in the blood, but may not be explicitly personal.

Table 7.66: Data Security — Process 5: Transmit Emergency Data

category	description	security level	coding
category 3	highly sensitive data II	intermediate	2

The data are assigned to the 3rd category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability of the SEGAL service, a minimum of seven participants can be assumed. The backend-system is regarded as being one participant/device.

Table 7.67: Scalability — Process 5: Transmit Emergency Data

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of "real-time". For process 5, the transmission of emergency data must be in real-time. In the SEGAL use case, the transmission of the AAL data in real-time must be possible in the event of an emergency.

Table 7.68: Real-Time — Process 5: Transmit Emergency Data

time	coding
1 s	0

The real-time is rated as 0.

Summary

The analysis yields the following definition for the role of "SEGAL": $\text{SEGAL}_{\text{transmit\_emergency\_data}} = (2,1,0)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (2,1,0).

7.5.3.7 Process 6: Transmit Analyzed Data

Data and Information

Process 6, transmit analyzed data, generates and transmits the following data and information: device ID, customer data ID, hub-ID, SMGW ID, analyzed data.

Participants

The following participants are involved in process 6: AAL-device, SMGW, SEGAL user, energy supplier, control center — medical service, backend-system.

Data Security

The data obtained are now evaluated with regard to data security on the basis of the defined criteria. No personal data are processed in process 6. Analysis data is transmitted after being made anonymous.

Table 7.69: Data Security — Process 6: Transmit Analyzed Data

category	description	security level	coding
category 1	non sensitive data	low	0

The data are assigned to the 1st category.

Scalability

The information identified is evaluated with respect to the participants in this section using the criteria for "scalability". Considering the scalability of the SEGAL service, a minimum of seven participants can be assumed. The backend-system is regarded as being one participant/device.

Table 7.70: Scalability — Process 6: Transmit Analyzed Data

participant	coding
$3 \leq 100$	1

The scalability is rated as 1.

Real-time

The process is now evaluated with regard to the criteria of "real-time". In process 6, the transmission of the anonymized data is not subject to any time restrictions. No real-time requirement is given.

Table 7.71: Real-Time — Process 6: Transmit Analyzed Data

time	coding
1 h	3

The real-time is rated as 3.

Summary

The analysis yields the following definition for the role of "SEGAL":
$\text{SEGAL}_{\text{transmit\_analyzed\_data}} = (0,1,3)$.

Selection — Security Measure

The mapping table refers to a security measure with the rating (0,1,2).

7.5.3.8 Summary: Use Case SEGAL

The evaluation of the SEGAL use case was based on the identified processes. The processes were appraised using the developed process model for security assessment. Table 7.72 summarizes the results.

Table 7.72: Summary — Use Case SEGAL

process	security assessment	security measure
process 1	2,1,2	2,1,1
process 2	2,1,2	2,1,1
process 3.1	2,1,2	2,1,1
process 3.2	1,3,3	1,2,2
process 4	2,1,2	2,1,1
process 5	2,1,0	2,1,0
process 6	0,1,3	0,1,2

Processes 1, 2, 3.1, and 4 are the same in the security assessment and describe the basic processes and the update of a single user. Process 3.2 differs mainly in the number of participants. In the case of system updates, all participants are affected. In process 5, emergency data are transmitted, influencing the real-time criterion. In process 6, however, anonymized data is transmitted, primarily reflected in the security evaluation. Figure 7.4 summarizes the results of the security assessment.

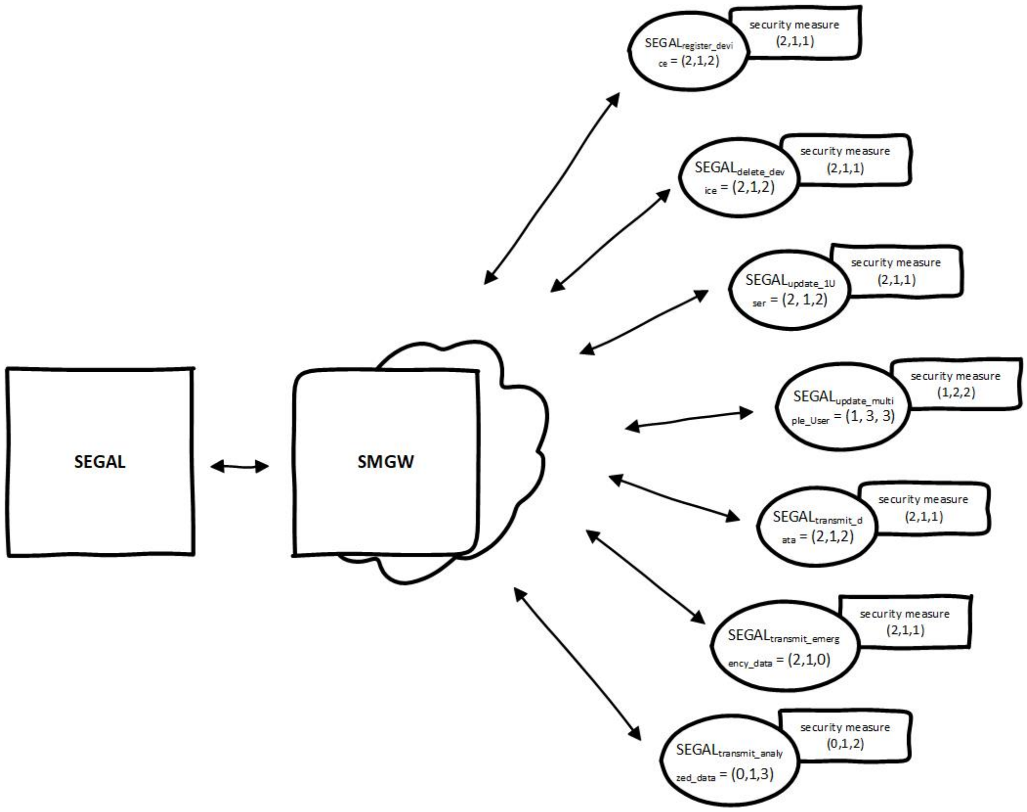
SEGAL
SMGW
SEGAL$_{register\_device}$ = (2,1,2)
security measure (2,1,1)
SEGAL$_{delete\_device}$ = (2,1,2)
security measure (2,1,1)
SEGAL$_{update\_1User}$ = (2, 1,2)
security measure (2,1,1)
SEGAL$_{update\_multiple\_User}$ = (1, 3, 3)
security measure (1,2,2)
SEGAL$_{transmit\_data}$ = (2,1,2)
security measure (2,1,1)
SEGAL$_{transmit\_emergency\_data}$ = (2,1,0)
security measure (2,1,1)
SEGAL$_{transmit\_analyzed\_data}$ = (0,1,3)
security measure (0,1,2)

Figure 7.4: Security Assessment Use Case SEGAL

7.5.4 Summary

In Chapter 7.5, the developed PROSA was presented using the example of a smart grid. The functionality of the framework was demonstrated based on the applications "smart metering", "feed-in and load management" and "SEGAL".

It has been shown that the developed framework works in application. A security evaluation concerning further aspects (scalability and real-time) is feasible and essential. Due to this exact evaluation, it is possible to select accurately adapted security measures.

For the classic use cases such as "smart metering" or "feed-in and load management", the added value of the new approach to security assessment can only be observed in the cases of an update. In contrast, the added value of the new approach can be observed in the "SEGAL" use case. Compared to the classical processes from the energy industry, the "SEGAL" use case imposes different requirements on the system.

The application example also shows that not every process has the same data security, scalability, and real-time requirements. This can be observed in

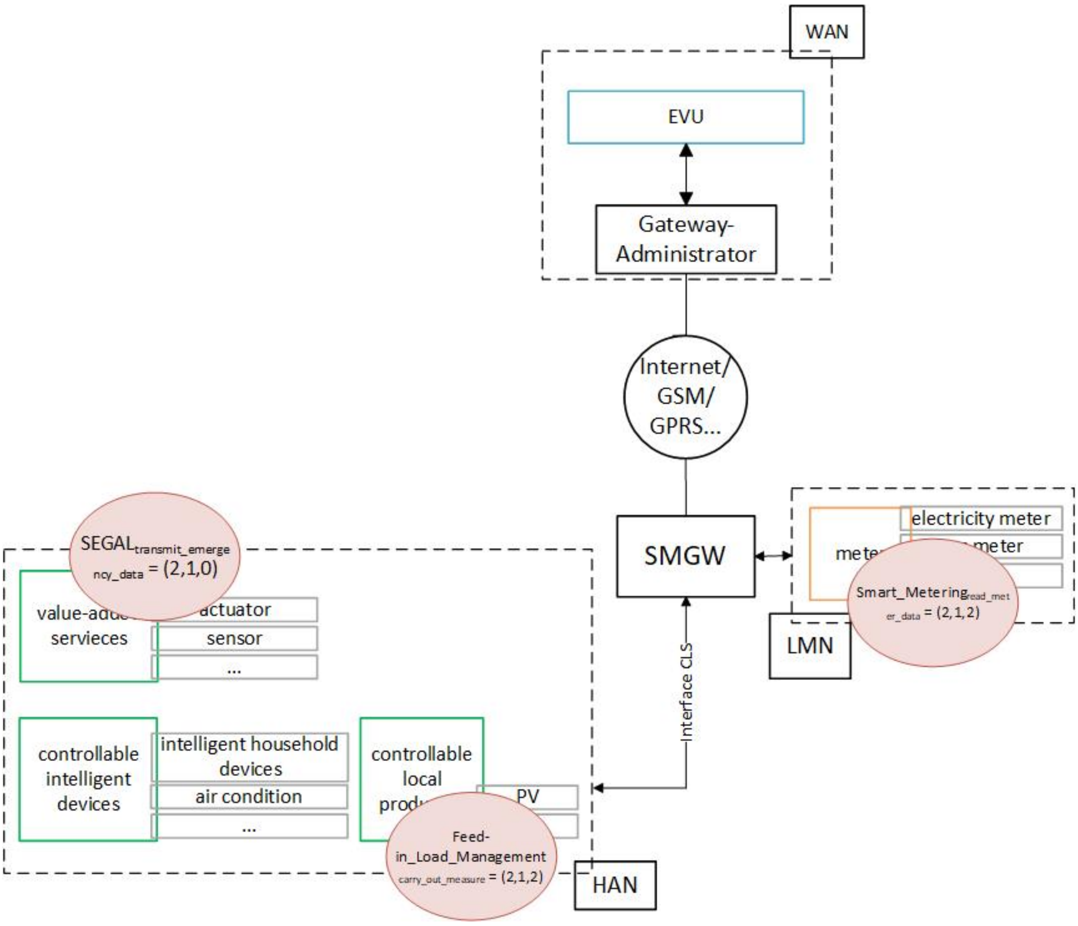
WAN
EVU
Gateway-Administrator
Internet/ GSM/ GPRS...
SMGW
Interface CLS
LMN
mete
electricity meter
meter
Smart_Metering read_meter_data = (2,1,2)
SEGAL transmit_emergency_data = (2,1,0)
value-add servieces
actuator
sensor
...
controllable intelligent devices
intelligent household devices
air condition
...
controllable local prod
PV
Feed-in_Load_Management carry_out_measure = (2,1,2)
HAN

Figure 7.5: Case Study Smart Grid: The Identical Security Assessment is not Given to Each Process

the following sample (see Figure 7.5). The “SEGAL” use case shows that the criteria of real-time is a justified extension of the classical model for security assessment. However, not every process requires real-time. This additional consideration allows the selection of more targeted measures. The importance of the scalability criterion is particularly striking in the case of update processes. The new classification of security is also reasonable. In the case study, it was shown that no personal data are involved in any of the processes.

As a final conclusion of the case study, it can be said that the developed process-oriented framework is applicable in practice and proves the applicability of the framework for security assessment in the smart grid. The results of this case study also mean that a statement can be made about the implementation of classical security assessments in CPS and an answer to the research thesis can be given. In future use cases of the smart grid, the classic security assessment will no longer be sufficient. The case study has shown that different data are processed, which justifies an adapted trust modeling. By adapting the evaluation criterion by means of a new trust model (4-Level-Trust-Model), an even better statement can be made about the security level. In the context of this case study it could also be shown that the evaluation criteria of scalability as well as a real-time requirement have their justification. There are classic processes where these criteria do not play a role. These criteria are particularly important in new and innovative processes. Thus, the application of the developed model is indispensable here since criteria such as scalability and real-time are becoming increasingly important. With the model I have developed, a new, innovative security assessment in CPS is possible, which provides the best security level. The security level not only reflects the criterion of data security, but also makes a statement about scalability and real-time. The framework describes a process-oriented approach, which considers the whole system. The model I have developed describes a unique approach to the holistic security consideration of CPS with a new trust modeling as well as the extension of the evaluation criteria.

Chapter 8

Proof of Concept

The process-oriented framework developed has been demonstrated theoretically using the SEGAL case study. It leads to the question of whether today's authentication architectures can still do justice to the new approach and guarantee the necessary level of security. Further challenges are the CPS systems themselves. In the Chapter "Proof of Concept", the technical implementation of the framework is shown with an application example. The realization takes place in the process "SEGAL". An architectural concept for the technical implementation will be developed and presented later. The technical implementation was carried out in the Laboratory for Information Security and Compliance of the Ostbayerische Technische Hochschule Regensburg with various investigations outlined in bachelor and master theses.

8.1 Process-Oriented Authentication for Cyber-Physical Systems

The new process-oriented approach to security assessment also creates new challenges in the implementation of security measures. These security measures must be selected and implemented according to the respective process evaluation. By means of the evaluation of the security measures, the requirements and challenges of CPS have already been taken into account. What is open here is the management of the security measures, which must be mapped on a process basis. In the management of the security measures, the requirements of CPS (for example, that they should be highly scalable) must be considered.

In the context of this work, the focus was placed on "authentication" when selecting the security measures. The process-oriented security assessment means that a new or adapted architecture must be developed for implementing the procedures. Existing procedures, such as a role-based access control model, cannot map the process-based approach in its entirety. In the known procedures, rights are always assigned to persons or users. For the process-based security assessment presented in this work, appropriate procedures for authentication must be developed or enhanced.

The selected authentication procedure in the smart grid with the technical implementation of PKI works in the classic application areas of the smart grid and by means of the known procedure for security evaluation. If we consider the smart grid in its foreseeable future dimension and as a CPS, the current procedure will reach its limits. The architecture puts the primary focus on security, at the expense of performance and speed. While the use of PKI provides a high level of security, performance is compromised because complex encryption algorithms must carry additional data during communication. This additional amount of data, also known as overhead, must be transported with the payload across the SMGW, resulting in a performance loss. Because of this performance loss, soft real-time requirements must be met in the best case. The more users are active in the system, the more overhead must be transmitted over the communication channel. Thus, the scalability criterion is also limited [74]. CPS generally have high requirements for security but also for scalability as well as real-time. If we look at the application example SEGAL (see Chapter 4.6.3), the model reaches its limits. The scalability and real-time requirements are important requirements in the SEGAL application example.

The proof of concept is intended to show that a process-oriented access concept for CPS meets the requirements of data security, scalability and real-time. The access concept describes an architecture that enables process-oriented access by means of various authentication procedures. The architecture to be developed is based on the basic idea that each process is implemented with a suitable authentication procedure depending on the requirements. For this purpose, the processes, as well as the authentication procedures, are evaluated on the basis of three criteria: data security, scalability and real-time. By assigning the authentication procedure according to the requirements of the process, a flexible model is created that meets the security assessment.

8.2 Design of Authentication Architecture

A use case consists of several processes and describes an application of the system. By analyzing the individual functions in more detail, it is possible to determine the security level of the data, the number of participating entities, and the time required for the particular use case. Based on these three characteristics of the respective use case, the system can be evaluated. The evaluation results are represented by a three-digit coding, where each digit stands for one of the following criteria: security, scalability, and real-time requirements. It is essential to understand that the coding does not conclude the use case since several use cases can get the same coding. A mapping table assigns the use case coding to the corresponding authentication procedures. This provides the link between the use case coding and the authentication method coding. Again, the result is represented by a three-digit coding, which is the common basis of the architecture. After the use of the authentication procedure, access may be gained to the required resource or communication channel.

The authentication architecture is based on the role-based access system. Role-based access control is about providing flexible resource management for individual users [75]. This authentication architecture is not about resource

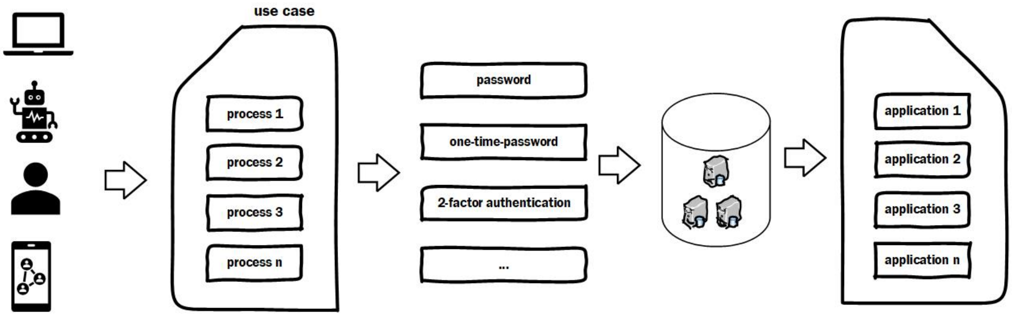

FIGURE 8.1: Overview — Technical Implementation

management but about the correct assignment of authentication procedures to particular use cases. The use cases are the equivalent of the individual users in the access model and are evaluated and classified into specific roles related to the criteria for data security, scalability, and real-time requirements. The resources in the role-based access control represent the authentication procedures in the architecture [74].

8.3 Proof of Concept: Secure Gateway Service for Ambient Assisted Living

The implementation of the simulation software can be roughly divided into three essential components. The client simulates the functionality of the architecture presented. In this context, it is the client of the RESTful web service. The client has access to the methods of authentication implemented by the RESTful web service via the interfaces implemented by the registration and login methods. The database component stores the user data, the passwords hashed and the certificate required for the PKI.

The implementation of the authentication architecture is a simulation and uses assumptions and specifications to represent the concept as realistically as possible. An example of this is the selection of processes to be evaluated. These are simulated by using a data structure designed to store and thereby represent the processes' data. A random process is chosen from the set, and then a case is chosen and used to represent the different occurrences of the process. Ultimately, the decisive events determining the cases chosen are also random in reality. The choice of process is implemented in the UseCaseFactory class. This generates an instance of the use case class with the specified attributes, i.e., the number of people involved, the security level of the data used, and the maximum time in seconds probably needed to execute the process.

Next, the evaluation table of the use cases is initialized. In each case, a table is created for security, scalability, and real-time requirements. The kind of data chosen is the HashMap. This makes mapping very easy with key and value pairs.

For the SecurityTable, the SecurityLevel Enum is used. Here, the SecurityLevel is the key assigned to unique encoding. The number of the coding is stored in an integer variable, which is transferred after evaluating the three criteria into the class Coding, then the CodeMappingTable is used. This is initialized first and filled with values. The CodeMappingTable is also a HashMap determining the assignment of authentication methods to processes, so an authentication procedure can be inferred from a process evaluation. Since the authentication method and its encoding relationship is 1-to-1, an authentication method can be chosen. Once the encoding of the authentication method has been obtained from the AuthMappingTable, this method can be determined and used. Since the simulation acts as a client, the implementation of the procedures is written as an http-request recognizable by the RESTful web service.

Each authentication method has its class and implements the authentication interface. The latter contains only this method, which specifies the method used by the request (GET, POST, PUT, DELETE), the URI to which the request must be sent, and the content to be sent. The content is passed as a JSONObject, since this defines the interface. The POST method is used here as much as possible since all methods require either a user-name, a password or a certificate name to be passed. These values must be given in JSON format, to let the web service handle them [74].

8.4 Summary

The architecture presented lets PROSA be implemented technically with the security measure “authentication”, as shown by using the SEGAL application as an example. The technical implementation shows that it can be used in practice. Implementing the SEGAL application shows that requirements in the form of data security, scalability and real-time influence each other. If data security has priority, the other two requirements are not met equally well.

The greater the security of data, the more complex the encryption algorithms, resulting in an increase in the data to be transferred. The more data is transferred, the slower the response times of the respective request. The response times are decisive for scalability and real-time requirements. If response times are longer, real-time requirements cannot be met. The more data that must be transferred per user, the more effort is needed by the system to transfer this data, so fewer users can use the service simultaneously, which is the definition of scalability. Conversely, the higher the performance or real-time requirements, the less secure the authentication procedure can be.

The result is that no authentication procedure can fulfill all three conditions simultaneously, since the conditions influence each other. In the current technical implementation in the smart grid, the communication unit SMGW was established. For this purpose, an authentication architecture was designed that uses the PKI with the Elliptic Curve Encryption Scheme. This architecture encrypts and authenticates the data transmission with the state-of-the-art encryption algorithm for the sake of securing data. This approach is quite suitable for classic use cases from the smart grid, as none of them call for scalability or real-time, but the situation changes as soon as the SEGAL use case communicates via the SMGW. The static authentication architecture of the BSI is then no longer sufficient to implement processes such as an emergency call since the PKI cannot adequately meet the real-time requirements.

As already described, no authentication procedure can satisfy all three criteria fully, but some procedures satisfy some criteria better than others. One of the solutions presented in this paper is to design a process-based authentication architecture that chooses the authentication procedure most suitable for any one use.

The proof of concept demonstrated a solution to the problem of authentication using process-oriented security assessment. An alternative architecture for authentication was presented, which enables a process-based selection of security measures using authentication as an example. This architecture can also be used to ensure future data flow as well as access to systems. The authentication concept developed in this thesis can also be used for further questions concerning the access concept. Not only can it be used for the technical implementation of measures in the context of a process-oriented security assessment, but also for use cases where, for example, a distinction is made between several procedures. The developed architecture is the best approach to implement process-oriented authentication measures.

Chapter 9

Analysis

The process-oriented framework was developed based on the identified criteria. It was tested on the basis of the smart grid case study, and a proof of concept was carried out with regard to the security measures. It is now necessary to verify whether the objectives of the model development have been achieved. In Chapter 9, PROSA is evaluated according to the requirements criteria for CPS. The evaluation criteria are security, scalability, and real-time. Finally, the results and relevance to CPS are summarized.

9.1 Requirements Criteria

The framework developed in Chapter 7 is evaluated in terms of the requirements criteria for this development. These requirements are revealed by analyzing the "CPS" and the use case "smart grid". Based on the specified requirement criteria of data security, real-time, and scalability, PROSA was developed and will be evaluated in terms of these criteria in the following chapter. The evaluation criteria are explained below.

Data Security
The framework is evaluated by using the criteria for data security defined in Chapter 7.1.1. Whether the data have been classified into the categories developed and whether this classification is justified will be checked. In particular, categories 2–4 are examined in greater detail since personal and sensitive data are transmitted. Attention must be paid to the possibility of personal reference. The evaluation is to be based on the "smart grid" use case.

As a second starting point, security measures (compare Chapter 7.3) have to be assigned according to the defined data security category. The security measures chosen should match the category.

This evaluation criterion is intended to refer to the topic of trust modeling with regard to the research context. The current state of the art modeling is not suitable for security assessment in CPS. An adapted trust modeling for the security assessment was defined on the basis of the identified requirements.

Scalability
The scalability criterion is checked by using the criteria defined in section 7.1.2.

It is evaluated on the basis of the key indicators (2, 100, 10.000, 10.001) represented while using the smart grid as an example of application.

As in the case of data security, the second starting point consists in assigning security measures (see Section 7.3) according to the defined scalability criteria.

Scalability is an identified requirement criterion from the requirements analysis of CPS. The approach to security assessment has been extended to include the evaluation criterion of scalability. Through this development step, the requirements of CPS are taken into account. With this additional evaluation criterion, a better statement can be made regarding the security level under the influence of scalability.

Real-time
The real-time requirement is evaluated by using the key figures defined in Section 7.1.3. The appropriate time units (1 sec, 1 min, 15 min, 1 h) from the smart grid application example are considered.

As in the case of data security and scalability, the second starting point consists in assigning security measures (see Section 7.3) according to the defined criterion for real-time.

Real-time is another identified requirement criterion of CPS. Real-time was mapped as the third evaluation criterion in the security assessment process. The security level can also be interpreted in terms of real-time through this development step.

9.2 Assessment of the Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

PROSA is assessed in terms of data security, scalability, and real-time. Firstly, it allows systems to be divided into processes, and then these are assessed in terms of the above requirements. On the basis of these assessments, there is a choice of security measures already assessed. PROSA itself is then assessed in terms of security, and the result determines the choice of an overall security measure. The technical implementation of the “smart grid” use case is also referred to in this context.

9.2.1 Data Security

Data security is increasingly becoming an essential building block when considering systems. In the case of CPS, there are data of various kinds, origins and quality. The classic data security assessment is insufficient for CPS since many anonymized, sensitive and personal data are processed here. The three-category approach (low, medium, and high) cannot be applied.

According to PROSA, the evaluation is classified into four categories. Here, a distinction is made between anonymized data, personal data. There are two classical categories for anonymous and genuinely personal data, and there are two categories for highly sensitive data I and II (4-Level-Trust-Model). The latter includes all other data, especially combinations of two or more, which allow conclusions about the user be drawn. This classification is no longer a classic division into secure and insecure but rather a data analysis based on needs. This ensures security measures are chosen according to needs.

Suppose PROSA is taken to be a practical application. The data is divided into these four categories in the smart grid use case for the first time. Data was formerly split into three categories, with data such as phase angles being put into the highest category, where, however, no personal reference can be established. In the application example from Chapter 7.5, for instance, personal data are assigned to category four (compare use case SEGAL). In the "device register" from the use case feed-in and load-management, data are assigned to category three. In the case of this data, two data in combination allows a user draw conclusions, but two data apart do not. In the previous approach, data in combination belonged in the high risk category, but as in the SEGAL example, data transferred anonymously belong in the low risk category.

With this assessment of the security of data, security measures can be issued specifically for the data processed but must be assessed beforehand in terms of "data security". A new view and process-related implementation have been shown to be useful in allowing measures to be tailor-made for the data. A process-related security assessment with fitting measures can be implemented in practice, as shown by the technical implementation of the SEGAL case study.

The novelty in the procedure of the evaluation of the data can be seen in the introduction of a new trust modeling. The evaluation of the data security does not take place as before by means of three categories, but with four categories. The need for protection of the two middle categories is evaluated by the possible inference to the user. By combining different data, conclusions can be drawn. This approach, which is innovative, means that only data relating to "real" persons is assigned to the category with the data requiring the highest level of protection. The second new approach can be seen as the evaluation of processes. In the approach developed in this work, use cases are represented in their atomic processes and evaluated with respect to data security on the basis of these. In addition to the security assessment, a new approach was also taken in the selection of security measures. The measures are also evaluated on the basis of data security. This means that targeted measures can be selected for each security level.

9.2.2 Scalability

Not only data security but also scalability influences the assessment of processes. One characteristic of CPS is that the systems can be described as rapidly growing. Furthermore, there is also an increasing number of participants. If a system with one participant is viewed alone, there is only a small limited system, but if a system with many participants is viewed as a whole, there is a big open system.

The assessment of scalability in accordance with PROSA can be divided into four categories. The assessment of the process takes place on the basis of key figures, as these reveal how many parts a process has in the system. This is a new approach to assessing security and ensures that security-measures are chosen according to needs.

If we look at PROSA in practice, we have to define the metrics. This is done by taking expected participants into account, as shown by the processes of updating. Fewer participants are involved in the "single user" update process than in the "multiple user" update process. When suitable security measures are being chosen, the possible scalability of a system must likewise be taken into account.

The technical implementation based on SEGAL's case study has shown that the means of authentication are not all scalable to the same extent. Measures can be chosen specifically to cover the exact needs of the process.

In addition to the new approach, the novelty of the developed process model lies in the expansion of the evaluation criteria. In addition to data security, this assessment model also considers scalability. In previous security assessment procedures, such as BSI IT Basic Protection, only data security was considered. With this extended security assessment, a new quality of statement can be made about the security level. Here, not only data security is considered, but also scalability. In context, this means that the security level is dependent on scalability, or vice versa. These dependencies only become apparent when suitable security measures are selected. As the proof of concept (see Chapter 8) has shown, if there is a need for a high level of security, then restrictions may have to be placed on scalability. This is also true in reverse. The framework developed in this thesis provides added value in the security assessment. The new approach makes it possible to make a statement about the data security factor in combination with scalability.

9.2.3 Real-Time

Real-time likewise influences the process of assessing a CPS. In looking at such a system, we can increasingly consider real-time criteria. Real-time plays an essential role in choosing measures suitable for data security and scalability.

Assessing the real-time in accordance with PROSA involves four categories. The processes are assessed on the basis of relevant figures from real-time, chosen according to use. This basis is essential in choosing security measures that do justice to real-time needs.

If we look at PROSA in practice, criteria related to applications have here been defined. In addition to real-time, an important key factor is the 15 min criterion, which is also anchored in law. As additional factors, 1 min and 1 h were specified. The real-time factor is of great relevance when choosing security measures. The different evaluations can be seen in SEGAL "transmit data" and "transmit emergency data". If the evaluation is, however, the same, the process analysis of the real-time requirement may represent the difference, so another, more suitable sighting measure may have to be chosen.

The technical implementation based on the SEGAL case study has shown that the authentication procedures have different response times in terms of real-time, so it is practical to use a process-related assessment, which explicitly evaluates the appropriate measures.

In addition to the innovations described so far, another new feature is that real-time has been included in the model as a further evaluation criterion alongside data security and scalability. This means that not only can a statement be made about data security in combination with scalability, it can also be extended to include real-time. Real-time is a requirement criterion that can be observed in CPS. The proof of concept (see Chapter 8) demonstrated the added value of this new approach. On the one hand, it could be established that not every atomic process of a use case leads to the same security assessment as a result. On the other hand, it could be shown that in the selection of appropriate security measures, the three criteria have a mutual interaction. For example, in the requirements of real-time, often high scalability or even high data security requirements can no longer be considered. The requirement of real-time is a significant criterion in the security evaluation of application areas of CPS. In particular, in application areas where sensitive data must be exchanged in real-time or near real-time, such as transportation and traffic.

9.3 Summary

PROSA has shown that process-oriented security assessment with the additional criteria of scalability and real-time provides added value. The application example showed that the three criteria were met and contributed to security assessments. As regards data security, the criteria for scalability and real-time are set on an application-specific basis, but these are generally divided into four categories.

Security measures can be chosen explicitly according to needs by looking deeper. The example of authentication showed the advantage of this, as no single authentication measure is the best choice for every process. The three criteria (data security, scalability, and real-time) must be considered harmoniously.

PROSA must be regarded as a process model that performs a systematic assessment. A systematic assessment is especially important for CPS, as these systems tend to change fast. A cycle of recurring consideration of security assessment and evaluation of security measures should be introduced together with the framework.

One challenge is the technical implementation of rights management. The process-related assignment of security measures creates an administrative burden, which increases with the size of the system. The question here is whether this increased administrative burden outweighs the current (simple security assessment) implementation. The entire smart grid use case is mapped in PKI's authentication example in the current implementation.

In general, it should be noted that the three criteria interact. This insight must be taken into account above all when choosing security measures. If data security is crucial, the need for scalability and real-time may not always be met, and the same is true of scalability. If scalability is crucial for a certain process, this may affect data security. Likewise, if real-time is crucial, this may affect data security and scalability.

If this finding is applied to the developed PROSA, there is need for weighting. Here, data security is weighted twice as much as scalability and real-time.

To conclude, the following key findings can be summarized:

- a model for security assessment that is process-oriented has been developed
- in addition to data security, the requirement criteria scalability and real-time have also been mapped in the security assessment
- data security evaluation criteria — a new type of trust modeling — has been redefined
- a procedure for the evaluation of security measures using authentication as an example has been developed
- a proof of concept with validation of the approach has been implemented.

These key results provide answers to the research question from different perspectives and provide a valuable contribution to the security assessment of CPS. The previously valid trust modeling needs to be adapted because CPS generate a variety of different data (compare Chapter 6). In the context of this development, a new proposal for data security assessment was developed, which is also mapped in practice by the case study as well as the proof of concept as a functional trust modeling. With the process-oriented approach, the requirements of CPS are taken into account, and a holistic view of the processes takes place. The consideration of further evaluation criteria enables a more detailed security assessment of CPS as well as a statement about the further requirement criteria of CPS. This new approach to security assessments has made it possible to realize that the selection of security measures must also be based on the three criteria. Thus, the most suitable measures can be selected for each process security assessment. An essential realization here is that the three evaluation criteria influence each other (compare Chapter 8). Within the scope of the work, a weighting was introduced for this problem, with an emphasis on data security.

The approach I have developed in this thesis represents a unique approach in the security assessment of CPS. For the first time, the use cases were described in atomic processes for the security assessment, and these were evaluated on the basis of the evaluation criteria data security, scalability and real-time. In the developed approach, the linking of the evaluated security measures with the security analysis can also be considered an innovation. This new approach to the selection of security measures represents a new challenge in the management of security measures. In the context of this scientific work, a proof of concept was accomplished on the basis of the security measure authentication in the application example SEGAL (see Chapter 8). As part of the proof of concept, an authentication architecture was developed that enables process-related authentication. This has the advantage that the most suitable procedure is used depending on the security assessment and not, for example, the most secure procedure generally. The developed process model for the security assessment of CPS represents a holistic approach.

Chapter 10

Added Value and Transferability

The process-oriented framework was developed using the smart grid as an application example. It represents an innovation in the security assessment of CPS systems. The framework was designed as a process-oriented framework. It can be adapted for use in other CPS application areas. Due to the process-oriented approach, the model can also be automated in parts. This is the basis for software-supported security assessment. This chapter outlines the added value of the use case smart grid and shows how the model might be automated and implemented in software. Furthermore, the model is applied in the field of automotive systems to show its necessity and functionality in other fields.

10.1 Added Value for Smart Grid

PROSA has shown its applicability in the case of the smart grid. The case study in Chapter 7.5 demonstrates the applicability of the framework. Furthermore, the case study clarifies that a new classification of data security is necessary. A differentiation must be made from the previous middle category. An additional category was introduced here. This category is defined by the possible combinations with further data and their possible inferences. The further criteria of scalability and real-time showed their necessity in the case study. Another aspect of the developed process model is the targeted selection of security measures that meet the requirements of the process.

The model allows security to be viewed holistically. The process model developed allows each smart grid use case process to be considered. In the classic approach, the analysis does not take place based on processes. Furthermore, with the classic security approach, it is possible to analyze only parts of the system.

The framework developed is dynamic, making it possible to adapt the evaluation scheme to the changing requirements. The developed model must be adapted to the necessaries depending on the application area. This makes it possible to adapt to the constantly changing requirements in CPS. Only the evaluation scheme for data security is generally valid and independent of the application-specific requirements.

In addition to the purely security consideration, other requirements such as scalability and real-time are also considered. Mutual interactions can be identified here. The criteria of real-time and scalability influence security. This new approach has the advantage of selecting security measures to fit precisely to needs.

This scientific work focuses on the topic of security assessment of CPS in the application area smart grid. Due to the further development of the original smart grid into a complex system (CPS), the procedures for security assessment and the included trust model must also be analyzed. It has been shown that the previously valid trust modeling, which forms the basis for any security assessment, will no longer be suitable in the future (compare Chapter 6). Using the smart grid as an example, it was possible to show that a large amount of data will be collected in the future, but that this data will not be classed as "particularly worthy of protection". The system itself can be regarded as a highly scalable and volatile system. Against this background, the classic security assessment must also be further developed. It is no longer sufficient to consider only the evaluation criterion of data security, but also others such as scalability and real-time. The application example in Chapter 7.5 as well as the proof of concept in Chapter 8 has shown that the model I have developed can be used in practice as a functional security assessment. Furthermore, it has also been shown that the processes received different security ratings as a result, thus justifying the new definition of trust modeling (evaluation criterion data security). The proof of concept also shows that the selected authentication method will reach its limits in the future smart grid (to be understood as CPS). With the process-oriented access concept, an alternative concept was developed, which implements the process-oriented selection of security measures. This concept ensures that, depending on the security level, a suitable procedure is to be implemented. This is also intended to reduce the effort involved in the current authentication concept in the smart grid.

The requirements analysis (compare Chapter 6.1) has shown that in future smart grids, the previously valid trust model as well as the security assessment in a practical application will lead to new challenges. These challenges are the data flow as well as the complexity of the future systems (compare Chapters 1.2 and 5). With the framework for the security assessment developed by me, a model has been developed on the basis of the requirements of CPS using the example of the smart grid. Through this step, a model was developed that meets the requirements. Considering the state of the art (see Chapter 6.1) and the requirements analysis of the smart grid (see Chapter 4), the process-oriented framework for security assessment and selection of security measures is a novel approach. With the new process model, a security assessment that can be adapted to the new requirements is carried out and thus meets the challenges of CPS.

10.2 Automation

This framework can be automated to assess and choose specific security measures. Automation describes the possibility that, for example, processes are evaluated by artificial systems. These artificial systems follow programs based on automata or decision trees [76]. Automation is also discussed in the context of digitization. By automating a process model, business and process flows do not have to be evaluated by hand.

The developed framework can be automated to assess and choose specific security measures. By automating the framework, operational processes can be optimized with regard to security assessment. Thus, there is the possibility of regularly and automatically reviewing the processes. This covers the life cycle of the processes and enables a regular, automated security assessment. With the framework developed in this thesis's context, the application area's relevant processes must be identified to automate the security assessment. For the automated security assessment, further information on data security, scalability, and real-time are required. For the automated data security assessment, information about the type of data must be available.

For the scalability criterion, the number of participants and for the real-time, the time condition must be given. As soon as this information is available, the security assessment can be automated, and the appropriate security measures can be selected (see Figure 10.1).

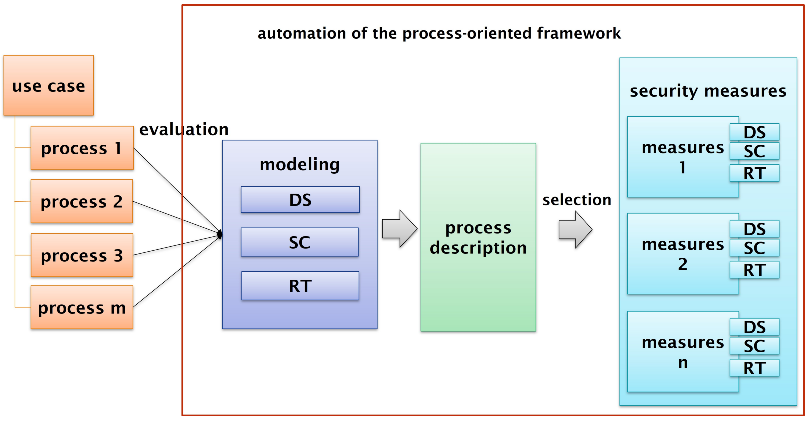

FIGURE 10.1: Automation of the Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

The automation of the model can be extended to include predictive analysis. In addition to security measures, it can also provide feedback on the further behavior of the process. For instance, this may involve providing guidance on scalability. High scalability, for example, may lead to a different selection of security measures. Furthermore, hints can also be given about what led to selecting the security measure and which criterion was dominant.

This can be done, for example, with the help of decision trees, whereby a decision tree stands in each case for the evaluation of a process in terms of a given criterion. Finally, a decision tree for security lets security measures be chosen. Figure 10.2 presents the process for evaluating data security as a decision tree. As a result, the decision tree provides the evaluation of the process in terms of data security.

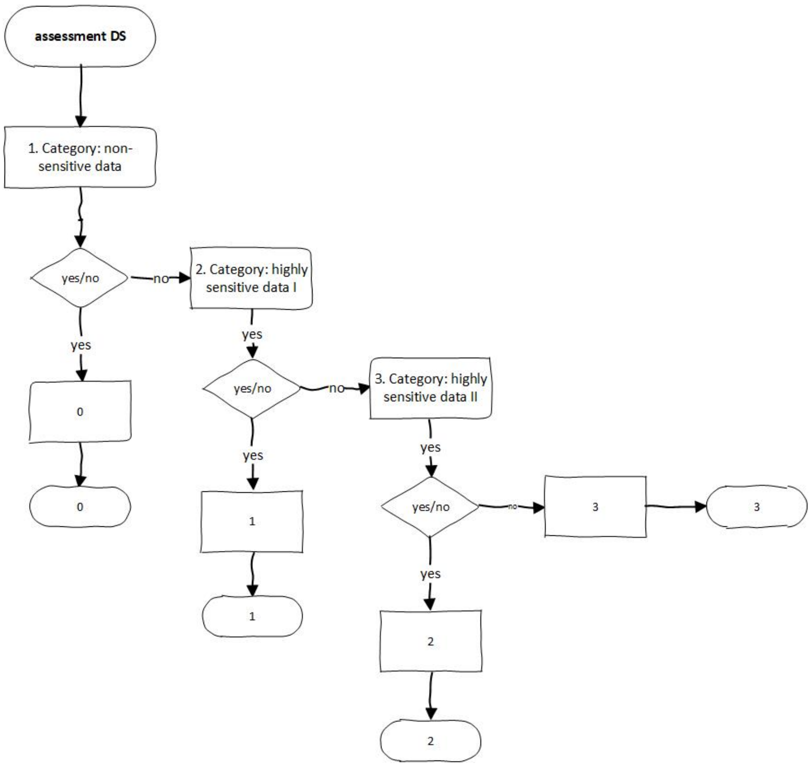
assessment DS
1. Category: non-sensitive data
yes/no
no
2. Category: highly sensitive data I
yes
0
0
yes
yes/no
no
3. Category: highly sensitive data II
yes
1
1
yes
yes/no
no
3
3
yes
2
2

FIGURE 10.2: Evaluation Criteria: Data Security

Figure 10.3 shows the process as a decision tree for scalability evaluation. As a result, the decision tree provides the evaluation of the process in terms of scalability.

The process for evaluating the real-time requirement is shown as a decision tree in Figure 10.4. As a result, the decision tree provides the assessment of the process with respect to the real-time requirement. The process for evaluating the selection of authentication measures is represented as a decision tree in Figure 10.5. As a result, the decision tree provides the selection of authentication measures. Figure A.1 shows PROSA as a completely automated process. The overall process is presented in Appendix A. This automated representation can also be used to develop a software-supported solution.

The model for the security assessment of CPS can also be automated, as is shown above. The automatability of the framework, was not a direct requirement. However, this can be presented as a side result. Due to the automated procedure, the model can be applied more easily in practice and can also be

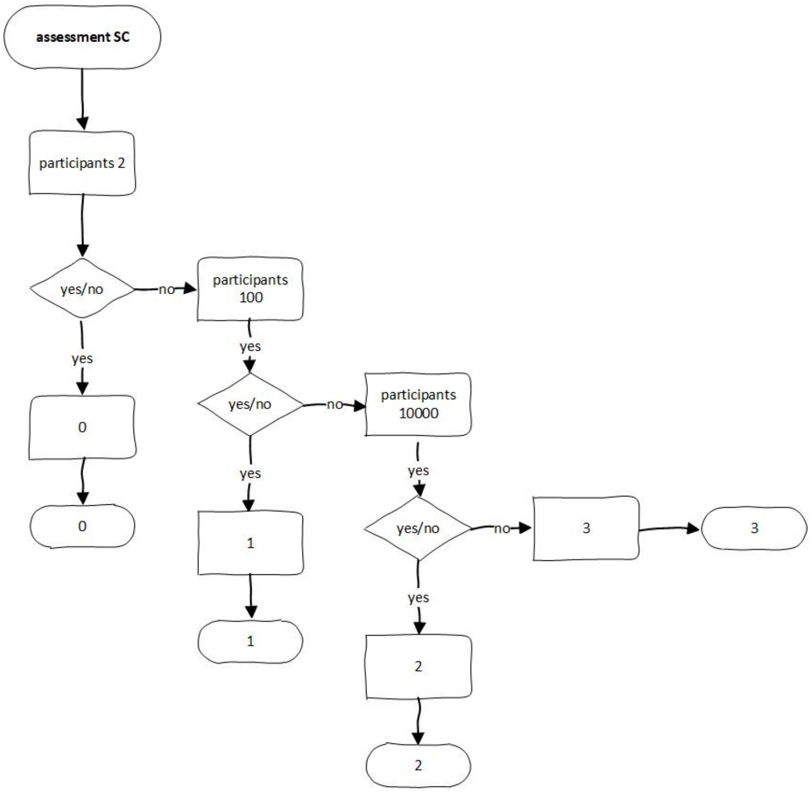

FIGURE 10.3: Evaluation Criteria: Scalability

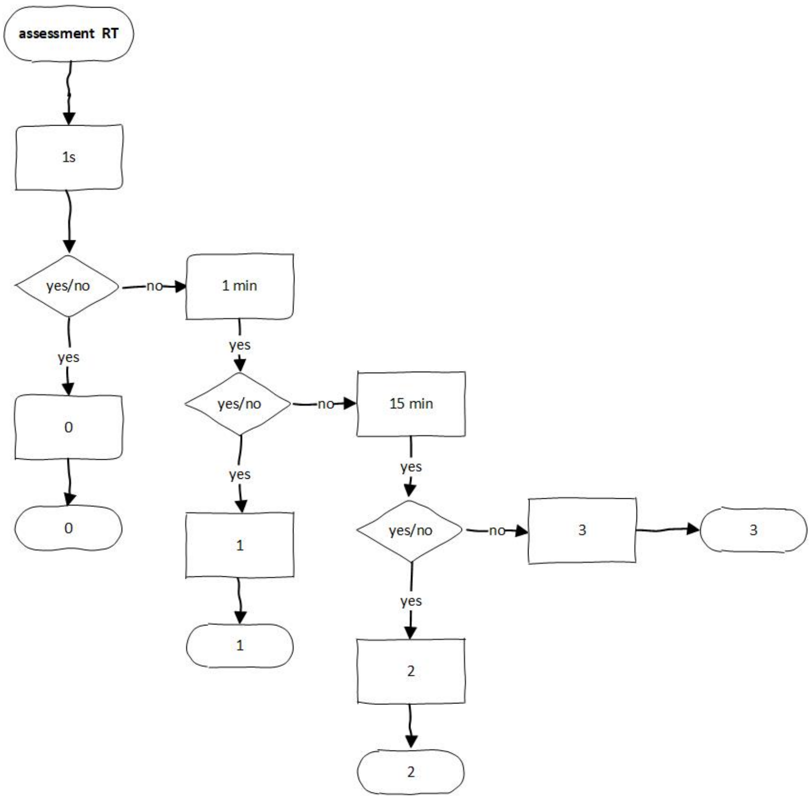

FIGURE 10.4: Evaluation Criteria: Real-Time

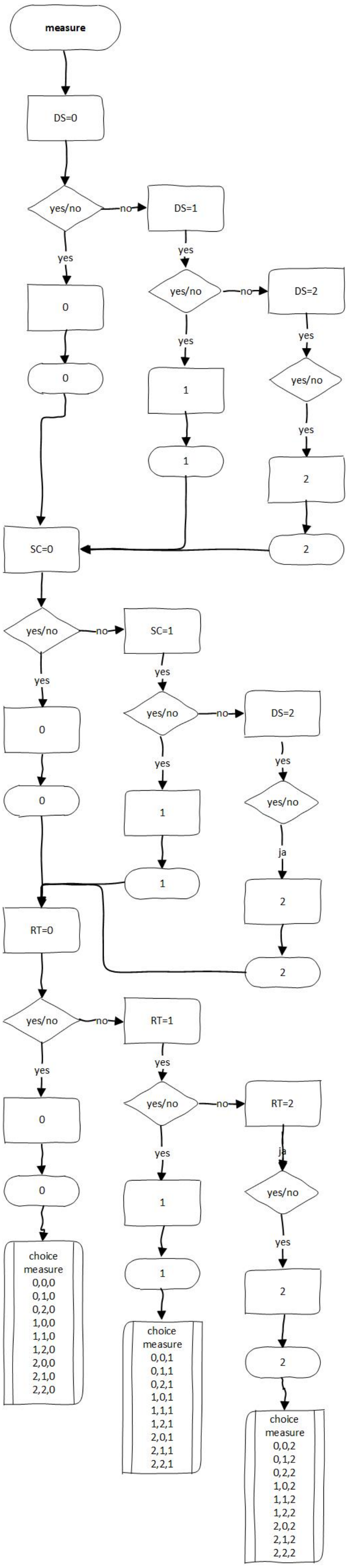

Figure 10.5: Selection of Security Measures

mapped tool-supported. Although the security assessment with the criteria of data security, scalability and real-time as well as the selection of security measures can be automated, the atomic processes with their properties have to be described manually, and the security measures have to be evaluated once. After analyzing the state of the art in science and technology, which was carried out to the best of our knowledge and belief, the automatable process-oriented procedure for the security assessment of CPS is considered to be an innovative approach.

10.3 Tool-Supported Security Assessment

The framework can be developed further as a tool-supported security assessment. The software solution would, in turn, be based on the three pillars of data security, scalability, and real-time requirement. To assess data security, existing solutions like verinice[1] could be adapted to the evaluation scale introduced in this work, and additional modules could be developed to meet the scalability and real-time requirements. Verinice implements the procedure according to BSI. For the choice of apt security measures, alternatives would have to be put forward and evaluated. For a new development of the software supporting solution, as already mentioned, all three pillars would have to be mapped, and the corresponding security measures would have to be shown automatically. The model developed in this work can be described as a process-oriented approach to security evaluation as well as an extension of the evaluation criteria to include scalability and real-time. The model developed here can be integrated into the BSI approach in two ways.

The classic BSI approach can be seen in Figure 10.6. In the BSI approach, a company's data, applications and systems are identified and evaluated in terms of data security. The evaluation with regard to data security is based on a risk analysis as well as the probability of occurrence and costs (compliance matrix). With the result of the security assessment, the security measures from the BSI compendium can be selected with the respective building modules.

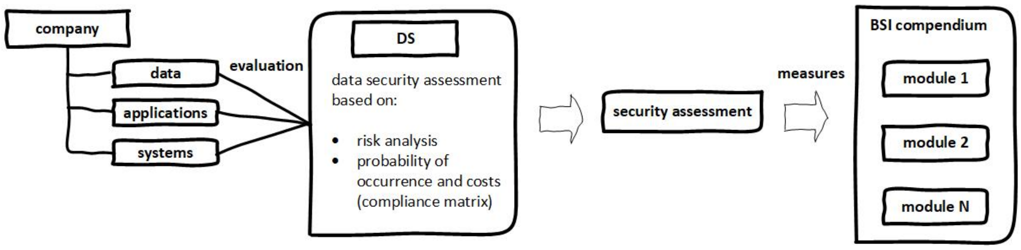

Figure 10.6: Modeling According to BSI

The first way of integrating the developed model can be done by extending the protection requirements assessment to include the criteria of scalability and real-time. The procedure for assessing data security must also be adapted. The

[1] www.verinice.com

evaluation criteria for data security must be expanded to include an additional category. Furthermore, the security measures catalog (BSI compendium) must be expanded with regard to the scalability and real-time criteria. With this possibility, the approach of the additional criteria is established also with the BSI procedure. This allows a more specific statement to be made with regard to the three criteria. In this approach to establishing the model, only the new approach to assessment is integrated. Here, the assessment of protection requirements is expanded to include the criteria of scalability and real-time, as well as the evaluation criterion of data security. The option to integrate the newly developed model does not describe a full implementation of the model. It only enables a more detailed statement of the security assessment with the aspect of scalability and real-time.

The second option describes an adaptation of the procedure and the integration of the developed assessment criteria. The process-oriented approach is integrated into the BSI procedure and the assessment of protection requirements is adapted on the basis of the evaluation criteria developed. The security measures (BSI compendium) are supplemented by the selection criteria of scalability and real-time. The integration of the process-oriented model developed as part of this work can be seen in figure 10.7 (shown in green).

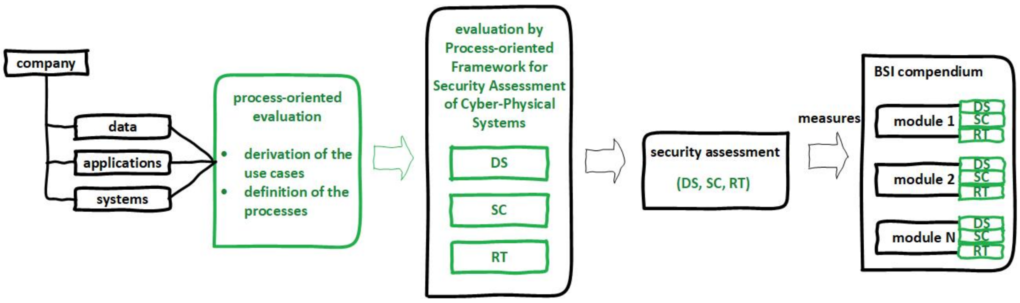
company
data
applications
systems
process-oriented evaluation
• derivation of the use cases
• definition of the processes
evaluation by Process-oriented Framework for Security Assessment of Cyber-Physical Systems
DS
SC
RT
security assessment
(DS, SC, RT)
measures
BSI compendium
module 1
module 2
module N
DS
SC
RT

FIGURE 10.7: Adaptation of the Modeling According to BSI by the Process-Oriented Framework for Cyber-Physical-Systems

The procedure according to BSI must be adapted as follows. After determining the data, applications and systems of a company, an intermediate step “process-oriented evaluation” must be inserted. In the process-oriented evaluation step, the use cases are derived and the processes defined. The next step is to determine the protection requirements using PROSA. Here, the processes are evaluated based on the assessment criteria of data security, scalability and real-time. The result of the security assessment is a statement about data security, scalability and real-time of a process, which is enriched with information from the first step. With the help of the security assessment, the appropriate measures can be selected from the BSI compendium. For this purpose, the measures must be evaluated in terms of data security, scalability and real-time.

When integrating the developed model, the second possibility, presented here, is to be preferred. In the second option, the entire model is integrated into the procedure. Through this, a security evaluation with the criteria of data security, scalability and real-time is carried out for each process.

The decision trees from Chapter 10.2 can be used as a basis to develop the tool-supported security assessment through the model. Therefore, the software can be used to perform an automated security assessment of processes. As already described in Chapter 10.2, the first step must be to determine the information regarding the identified processes. Here, the question must be clarified, which processes can be identified at all.

In a second step, information must be requested for the evaluation criterion of data security. What data is to be transferred? For example, personal data, data without personal reference or anonymized data, system data, etc. Likewise, information must be collected for the scalability criterion. Which participants exist, etc.

For the criterion of real-time, information must be collected about the time conditions, for example, real-time or, as in the application example, concrete time specifications (15 min). After entering and collecting this data, an automated security assessment can be performed. For this purpose, the evaluation scheme must be stored in the software. The corresponding security measures are displayed as soon as the security assessment has been successfully completed.

As presented in this chapter, the process-oriented framework for security assessment can be mapped for CPS as well as for tool-based software. The tool-supported security assessment can be seen as an additional option of the framework. Due to this feature, framework's application could be extended in the future. For the successful establishment on the market, this is an important feature. A further advantage is that the framework developed by me can be adapted into existing software tools, like Verinice. In order to implement the process model in its entirety, a new development must be carried out.

10.4 Abstraction of the Process-Oriented Framework

This framework was developed for CPS on the basis of the smart grid example of application. Depending on the field of application, the requirement criteria of scalability and real-time must be adapted. The assessment criteria for data security could already be standardized and applied in every field of CPS.

The new procedure for evaluating data security (4-Level-Trust-Model — classification into four categories) has been developed independently of application examples. The classification into the four categories has already been generalized and can therefore be used in any application area of CPS. The model for evaluating data security was outlined in Chapter 7.1.

The criteria of scalability and real-time (see Figure 10.8) must be determined for the area of application and be divided into the four categories. Reference can be made to legal framework conditions or to company-related values.

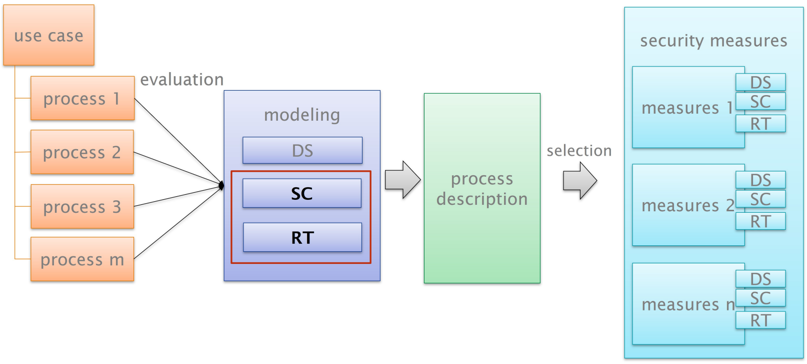

Figure 10.8: Abstraction of the Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

The further criterion of scalability must be adapted according to the application area. The classification should also consist of four categories. In the first category, the smallest, as well as the largest possible version of the system, should be examined. The second category usually refers to the requirements for classical processes. The third category can be understood as an average of categories two and four. For comparison, the scalability of the smart grid application in Chapter 7.1 can be considered.

The criterion of real-time must also be adapted depending on the field of application. The classification should also consist of four categories. Category one describes the real-time requirement of the system. Depending on the area of application, this is defined differently. The fourth category describes the most prominent possible factor of the criterion of time. Categories two and three are to be selected equivalently as with the scalability. Category two describes the classical use cases. As already mentioned, the framework conditions can be taken from the compliance requirements and service level agreements. The real-time of the smart grid application example in Chapter 7.1 can be considered as a comparative example.

Security measures do not have to be assessed again, as they were evaluated independently of the application example. The evaluation scheme of the security measures can be adopted for further evaluation of these. The evaluation is done without reference to a use case. The general derivation of the scheme can be understood in Chapter 7.2.

PROSA developed in Chapter 7.1 was developed on the basis of the required criteria for CPS and the smart grid application example. The research objective was to develop a generally applicable process model for security assessment for CPS. This chapter shows how the framework can be generalized. The evaluation criterion of data security was considered a universally valid criterion and was defined independently of the application example during development. The scalability and real-time evaluation criteria need to be adapted depending on the application domain. This offers the best approach for evaluating the criteria since these are always dependent on the respective application area. This type of approach represents a unique approach to the security assessment of CPS. New features are, besides the new definition of the criterion data security, the inclusion of the further evaluation criteria scalability and real-time. The evaluation of the security measures carried out in the context of this scientific work can be regarded as generally valid.

10.5 Applicability in Further Sectors

This framework can be applies in all areas of CPS, such as critical infrastructure, transport, or logistics. PROSA is shown in excerpts based on the example "autonomous mobility".

Autonomous Mobility - an Application Example

Autonomous mobility or digital driving is another domain of CPS where PROSA can be applied. The following processes from this area have been chosen for assessment.

- security update
- update maps
- transmission analysis data
- communication car-to-x
- communication car-to-traffic light
- communication car-to-car
- communication car-to-insurance
- communication car-to-parking guidance system
- communication car-to-emergency call
- communication car-to-manufacturers

Criteria for the Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

The evaluation criteria were adapted to the "autonomous mobility" use case. The data security remained unchanged, as it was generally valid, but the criteria for scalability and real-time were adapted to the application example. The basis for the evaluation criteria can be taken from the following tables.

Data Security

The evaluation scheme for data security has been taken from Chapter 7.1. As already explained, the evaluation scheme for data security has already been generalized and can therefore be adopted without adaptation.

Table 10.1: Criteria Data Security

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

Scalability

The evaluation criterion of scalability must be adapted to the use case. The classification was made with the threshold values of 2 participants, 10 participants, 1000 participants, and more than 1000 participants.

Table 10.2: Criteria Scalability

participants	coding
≤ 2	0
$3 \leq 10$	1
$11 \leq 1.000$	2
≥ 1.001	3

Real-Time

The criterion of real-time must be adapted to the application. The limit values are 1 ms (real-time), 2 ms, 1 sec, and greater than one second.

Table 10.3: Criteria Real-Time

time	coding
1 ms	0
2 ms	1
1 sec	2
$>$ 1 sec	3

Autonomous Mobility - Process-Oriented Framework for Security Assessment of Cyber-Physical Systems

The cases of use outlined above were assessed using PROSA. A description of each process was identified by using the criteria of data security, scalability, and real-time requirements, and the security measure was derived from the process description. The results are summarized below.

Table 10.4: Assessment Autonomous Mobility

process	**security assessment**	**security measure**
security update	2,3,0	2,2,0
update maps	0,3,0	0,2,0
transmit analysis data	0,3,3	0,2,2
communication car-to-X	2,3,0	2,2,0
communication car-to-traffic light	2,2,0	2,1,0
communication car-to-car	2,1,0	2,1,0
communication car-to-insurance	2,1,3	2,1,2
communication car-to-parking guidance system	2,1,0	2,1,0
communication car-to-emergency call	3,1,0	2,1,0
communication car-to-manufactures	2,3,0	2,2,0

Security Update

Data security was rated with 2. No personal data was transmitted. Data was transferred where the combination of two allowed conclusions about the user to be drawn. The scalability was rated as 3. This process involved a high level of scalability, as the whole system was affected. The real-time was evaluated as 0. The process security update included the request in real-time.
As can be seen, the security was assessed with (2,3,0) and the measures derived from this were evaluated with (2,2,0).

Update Maps

Data security was rated with 0. No personal data or data, enabling conclusions to be drawn about a user, was transmitted. The scalability was rated as 3. This process involved a high level of scalability, as the whole system was affected. The real-time was evaluated as 0. The process security update included the request in real-time.
As can be seen, the security was assessed with (0,3,0) and the measures derived from this were evaluated with (0,2,0).

Transmit Analysis Data

Data security was rated with 0. No personal data or data letting conclusions be drawn about a user was transmitted. The scalability was rated as 3. This process involved a high level of scalability, as the whole system was affected. The real-time was evaluated as 3. The Transmit Analysis Data process had no real-time or timing requirements.
As can be seen, the security was assessed with (0,3,3) and the measures derived from this were evaluated with (0,2,2).

Communication Car-to-X

The data security was rated with 2. No personal data was transmitted. Data was transferred; even when a combination of two data lets conclusions be drawn. The scalability was rated as 3. This process involved a high level of scalability,

as the whole system was affected. The real-time was evaluated as 0. The car-to-x process included the real-time requirement.
As can be seen, the security was assessed with (2,3,0) and the measures derived from this were evaluated with (2,2,0).

Communication Car-to-Traffic Light

The data security was rated with 2. No personal data was transmitted. Data was shared; even when combining two data let conclusions be drawn. The scalability was rated as 2. This process involved a high level of scalability, but the system as a whole was not affected. The car communication system was extended by the traffic light system. The real-time was evaluated as 0. The car-to-traffic light process included the real-time requirement.
As can be seen, the security was assessed with (2,2,0) and the measures derived from this were evaluated with (2,1,0).

Communication Car-to-Car

The data security was rated as 2. No personal data was transmitted. Data was shared; even when a combination of two data lets conclusions be drawn. The scalability was rated as 1. This process involved a low level of scalability. Communication took place from car to car. The real-time was evaluated as 0. The car-to-car process included the real-time requirement.
As can be seen, the security was assessed with (2,1,0) and the measures derived from this were evaluated with (2,1,0).

Communication Car-to-Insurance

The data security was rated as 2. No personal data was transmitted. Data was shared; even if combining two data let conclusions be drawn. The scalability was rated as 1. This process involved a low level of scalability. Communication took place between the car, insurer, and manufacturer. The real-time was evaluated as 3. The car-to-insurance process does not included a requirement of real-time. The data could be transmitted according to the schema.
As can be seen, the security was assessed with (2,1,3) and the measures derived from this were evaluated with (2,1,2).

Communication Car-to-Parking Guidance System

The data security was rated as 2. No personal data was transmitted. Data was transmitted; even when a combination of two data lets conclusions be drawn. The scalability was rated as 1. This process involved a low level of scalability. Correspondence occurred between the car, parking guidance system, and manufacturer. The real-time was evaluated as 0. The process car-to-parking guidance system included the requirement of real-time.
As can be seen, the security was assessed with (2,1,0) and the measures derived from this were evaluated with (2,1,0).

Communication Car-to-Emergency Call

The data security was rated as 3. Personal data was transmitted. The scalability was rated as 1. This process involved low scalability. Communication occurred between the car, the control center, and the manufacturer. The real-time was evaluated as 0. The car-to-emergency call process included the real-time request.
As can be seen, the security was assessed with (3,1,0) and the measures derived from this were evaluated with (2,1,0).

Communication Car-to-Manufactures

The data security was rated as 2. No personal data was transmitted. Data was transferred; even when combining two data let conclusions be drawn. The scalability was rated as 3. This process involved a high level of scalability because the whole system was affected. Communication took place between the car and the manufacturer. The real-time was evaluated as 0. The car-to-manufactures system process included the real-time requirement.
As can be seen, the security was assessed with (2,3,0) and the measures derived from this were evaluated with (2,2,0).

Summary

The security of "autonomous mobility" can be assessed by using PROSA. Indeed, the example shows that a process-oriented approach is advantageous. Here, a special assessment was made for each process. This example also shows that the criteria of scalability and real-time are justified. It could be shown that some applications have real-time requirements and others do not. The same applies to scalability: some processes affect the whole ecosystem, and others only map parts.

In this chapter, it was shown that the model can also be used in other application areas of CPS. Based on Chapter 10.4, the process model for the security assessment of CPS was adapted to the "autonomous mobility" application example. For this purpose, the evaluation criteria scalability and real-time were adapted to the example. Within the scope of this chapter, a proof of concept was developed, which proves the generalization as well as the use in other application areas. This has further shown that it is the best approach for the security assessment of CPS with further evaluation criteria (scalability and real-time) as well as the adaptation of the evaluation criterion of data security.

Chapter 11

Conclusion and Future Work

This thesis is about security assessment in a CPS. Discussions and questions about security are increasing, even regarding a CPS, which is a further development of systems, private or industrial. CPS are highly scalable and volatile and increasingly involve the processing of personal data. Known security assessment models no longer suffice for these systems. A modular approach is needed to cover the requirements of security assessment. Within the scope of this work, PROSA has been developed. This framework has been adapted to the requirements of data security, scalability, and real-time then used to perform a process-oriented security assessment of a CPS. These three criteria for CPS were determined in the context of the thesis. The resulting procedure is as follows: The use cases are divided into atomic processes, which are then described and assessed in terms of data security, scalability, and real-time requirements. This assessment can then be used to choose specific security measures, which must be classified in terms of the requirements of data security, scalability, and real-time.

In Chapter 7.1, I developed a process model that performs process-oriented security assessments in CPS and provides information about the security level with the influence of scalability and real-time. With this new approach, security measures can be derived. It describes a procedure that can be automated and is a prerequisite for tool-supported security assessment. The requirement criterion of data security describes four categories (4-Level-Trust-Model) in this process model. In the case of CPS, it is no longer sufficient to categorize data as either secure or insecure (trust model). In CPS, data differing in origin, quality and quantity are processed, so data has to be put into four categories, the new categories being anonymous data and personal data. The data is evaluated according to two or more possible inferences in these categories.

As already described, CPS are highly scalable and volatile and used in areas where real-time is required. These additional scalabilities and real-time requirements have also been mapped in PROSA. They must be determined according to the area of application. With PROSA, it is now possible to assess the security of a CPS system. It describes a process that must be reiterated to take continually changing requirements into account.

The process-oriented framework for security assessment is a new approach in the field of security assessment in CPS. Assuming the state of the art in science and technology in Chapter 6.1, the developed framework can be seen as an innovation. It differs to the previous approach. With the framework, a process-oriented security assessment is performed. This means that atomic processes are considered in the security assessment. A key feature is the new trust modeling for the data security criterion (4-Level-Trust-Model) and the establishment of the additional assessment criteria (scalability and real-time). Previous approaches to security assessment focus only on data security. PROSA describes an approach to security assessment that is innovative.

In Chapter 7.5, the framework was demonstrated using the smart grid as a practical example. A security assessment in the area of application "smart grid" was shown, revealing that the three required criteria have a reciprocal effect. If the security of data is crucial, this may compromise the requirements for scalability and real-time; if scalability is crucial, this may compromise the requirements for data security and real-time; and if real-time is crucial, this may compromise security and scalability. An increased requirement for one criterion affects the other criteria. For this reason, the criterion of data security was given twice the importance since the focus of the framework is on security.

Deployment areas of a CPS that have been evaluated according to PROSA can implement an individual authentication process, as this work has shown. Chapter 8 shows a new approach regarding a process-oriented authentication architecture. This process enables access, depending on the assessment and subsequent assignment of an apt authentication measure to a process. Through this process-based authentication, the minimum requirement for security is guaranteed according to the requirements of the process. In the case of conventional procedures, maximum security usually applies (compare current implementation of smart grid PKI). This implementation increases the effort required to manage access, but the advantage of being able to adapt a system to needs more than compensates for this.

In Chapter 9, the framework was analyzed with regard to the requirements. The most important result was the development of a process-oriented framework for security assessment. However, the process of security assessment was extended by the criteria of scalability and real-time and data security was adapted by means of a new trust modeling. In order to select measures that are fair to the corresponding security level, an approach for the evaluation of security measures was developed using authentication as an example. The case study as well as the proof of concept delivered best results in the testing of the framework.

Chapter 10 refers to the added value and transfer potential of the developed model for process-oriented security assessment. The developed model represents added value in the security assessment of smart grids. It provides the best results in security assessment by revising the data security assessment criterion and by adding scalability and real-time criteria. It also shows that the process-oriented concept for authentication is needed in the smart grid application example. Furthermore, PROSA can be shown to be automated. Both the security assessment as well as the selection of measures can be automated and this can be seen as a prerequisite for tool-supported security assessment. The tool-supported PROSA can represent a new development in the sense of the developed approach or can be integrated into existing solutions in an adapted way. PROSA was developed on the basis of the requirement criteria of CPS and the application example smart grid. The requirement for the development was to develop a generally applicable procedure for security assessment. The evaluation criterion of data security has already been developed as a generally applicable criterion. The evaluation criteria of scalability and data security must be adapted depending on the application area. The applicability in further application areas of CPS is shown in the example “autonomous mobility”. This proves that the framework for process-oriented security assessment not only provides the best results in the smart grid, but also the best results in this application area.

PROSA must be extended to include other criteria. It has been shown that extending the security assessment is useful to in making apt assessments and recommendations of measures for a specific CPS, and more work is still needed for assessing security measures. In this thesis, the procedure was illustrated by only one example of authentication. However, other security measures implemented as part of security assessments must also be classified, and, as such, the catalog of measures for PROSA must be extended.

It has been shown that the extension of the security assessment is advantageous. This extension will make fit-for-purpose security assessments and security measure recommendations for CPS. Further work is also required in the evaluation of security measures. In this thesis, the procedure was only shown using the authentication example. However, other security measures are implemented as part of security assessments. These further security measures must also be classified, and thus the catalog of measures for PROSA can be extended.

The process-oriented framework can be used in practice and delivers the best results in terms of security levels. In order to obtain even more optimized statements from the security assessment, the process model should be extended to include other required criteria. As was shown above, further security measures must be classified. The basic model developed here can be used for initial security assessment in companies. In order to increase the acceptance of the model with authorities and companies, the process-oriented framework should be established as a “defacto standard”. As a first step toward establishing it as a standard, industry associations can support it by using the process model as an alternative model.

In future technological and regulatory developments, the framework developed in the thesis can make a contribution. The framework developed here was based on the requirements of CPS. The areas of application of CPS cover a wide spectrum. It can be assumed that these application areas will constantly evolve and new application areas will be assigned to CPS. In order to perform a security assessment adapted to the changing challenges, the framework developed here can be used. It was conceptualized based on the requirements of CPS and implemented as a process-oriented approach. Further technological development also entails further regulatory developments. In future regulatory developments, PROSA can be used as a reference model for security assessments. This model can be referred to, for example, in technical guidelines, standards or also in instructions for action. With the developed framework, it is possible to perform security assessments for CPS according to requirements. The process-oriented framework developed in this work is the best approach for security assessments of future highly scalable and volatile systems.

To conclude this scientific work, there is clearly a need for a new approach to security assessment in CPS. In this thesis, I have showed that the framework developed is an innovation in the field of security assessment in CPS. It describes a process-oriented framework, which determines a security assessment under the influence of scalability and real-time. On the basis of this security assessment, precisely fitting security measures can be determined. This process model can be used to guarantee security in CPS. PROSA describes a unique approach for a holistic process-oriented security assessment for CPS.

Appendix A

Automation Entire Process

Figure A.1 shows PROSA as a completely automated process based on the SEGAL application example (see Chapter 7.5.3).

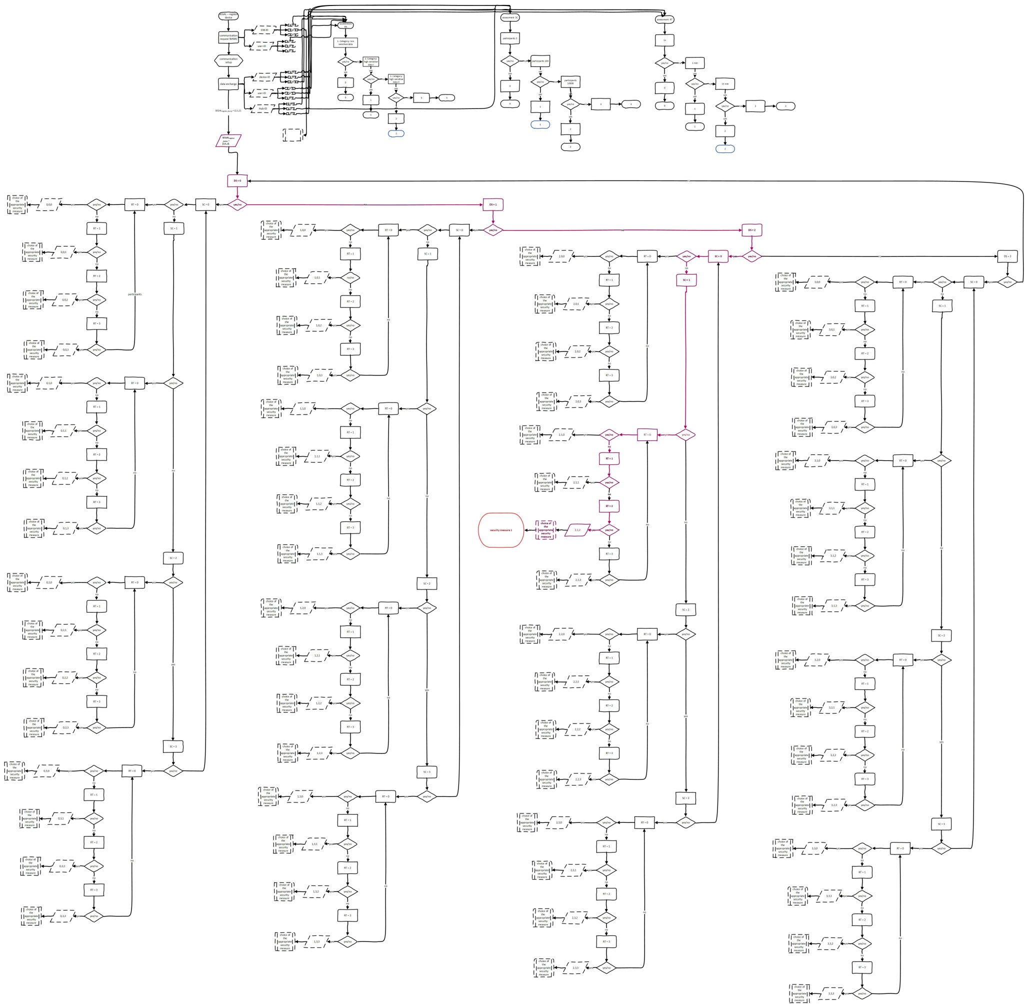

FIGURE A.1: Entire Process

Appendix B

Publications

The following related publications were published during this work:

- K. Neubauer, R. Hackenberg (2020)
  Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems
  (CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization) [9]

- K. Neubauer, S. Fischer, R. Hackenberg (2020)
  Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT - 4-Level-Trust-Model as a Security Solution
  (International Journal On Advances in Internet Technology, v 13 n 1&2 2020) [1]

- K. Neubauer, S. Fischer, R. Hackenberg (2019)
  Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT
  (ARCS 2019 - 32nd International Conference on Architecture of Computing Systems) [8]

- K. Neubauer, S. Fischer, R. Hackenberg (2019)
  Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things
  (CLOUD COMPUTING 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization) [7]

Bibliography

[1] Katrin Neubauer, Sebastian Fischer, and Rudolf Hackenberg. “Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT-4-Level-Trust-Model as a Security Solution”. In: *International Journal On Advances in Internet Technology* 35 (2020), pp. 11–20.

[2] Maximilian Irlbeck. “Digitalisierung und Energie 4.0 – Wie schaffen wir die digitale Energiewende?” In: *Springer Fachmedien Wiesbaden GmbH* (2017), pp. 135–148.

[3] Radhakisan Baheti and Helen Gill. “Cyber-physical Systems”. In: *The impact of control technology* 12.1 (2011), pp. 161–166.

[4] Mathias Uslar and Jörn Trefke. “Applying the Smart Grid Architecture Model SGAM to the EV Domain.” In: *EnviroInfo*. 2014, pp. 821–826.

[5] Ernst u. Young GmbH. *Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler*. 2013. URL: `https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kosten-nutzen-analyse-fuer-flaechendeckenden-einsatz-intelligenterzaehler.pdf?__blob=publicationFile&v=5`. (accessed: 07.2013).

[6] Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorfer Kreis. *Orientierungshilfe datenschutzgerechtes Smart Metering*. 2012. URL: `https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Orientierungshilfe_SmartMeter.pdf?__blob=publicationFile&v=2`. (accessed: 09.2020).

[7] Katrin Neubauer, Sebastian Fischer, and Rudolf Hackenberg. “Infrastructure of Smart Grid and Internet of Things”. In: *CLOUD COMPUTING, International Conference on Cloud Computing, GRIDs, and Virtualization* (2019), pp. 82–87.

[8] Katrin Neubauer, Sebastian Fischer, and Rudolf Hackenberg. “Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT”. In: *ARCS Workshop, 32nd International Conference on Architecture of Computing Systems* (2019), pp. 1–6.

[9] Katrin Neubauer and Rudolf Hackenberg. “Development of a Process-oriented Framework for Security Assessment of Cyber Physical Systems”. In: *CLOUD COMPUTING, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization)* (2020), pp. 38–43.

[10] Marc Elsberg. *BLACKOUT-Morgen ist es zu spät: Roman*. blanvalet Verlag, 2012.

[11] David M Nicol. “Angriff auf das Stromnetz”. In: *Unsere digitale Zukunft*. Springer, 2017, pp. 185–193.

[12] Torsten Eymann and Beatrix Semba. "Auswirkungen der Digitalisierung auf die Datensicherheit". In: *Herausforderungen für Familienunternehmen.* Nomos Verlagsgesellschaft mbH & Co. KG. 2020, pp. 21–28.

[13] Thomas Schneider. "Datensicherheit". In: *Digitalisierung und Künstliche Intelligenz: Einsatz durch und im Controlling.* Wiesbaden: Springer Fachmedien Wiesbaden, 2022, pp. 5–12.

[14] Claudia Eckert. *IT-Sicherheit.* Berlin, Boston: De Gruyter Oldenbourg, 2018.

[15] Dirk Loomans, Manuela Matz, and Michael Wiedemann. "Anforderungen an den Datenschutz". In: *Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems.* Springer, 2014, pp. 7–20.

[16] Vassilis Dimopoulos et al. "Approaches to IT Security in Small and Medium Enterprises." In: *AISM.* Citeseer. 2004, pp. 73–82.

[17] Ferrucio de Franco Rosa, Mario Jino, and Rodrigo Bonacin. "Towards an Ontology of Security Assessment: A Core Model Proposal". In: *Information Technology-New Generations.* Springer, 2018, pp. 75–80.

[18] acatech — Deutsche Akademie der Technikwissenschaften. *Cyber-Physical Systems: Innovationsmotor für Mobilität, Gesundheit, Energie und Produktion.* Springer, 2011.

[19] Bernd Becker. "Cyber-physisches System". In: *Mensch-Maschine-Interaktion.* Springer, 2019, pp. 247–249.

[20] Yosef Ashibani and Qusay H Mahmoud. "Cyber physical systems security: Analysis, challenges and solutions". In: *Computers & Security* 68 (2017), pp. 81–97.

[21] Oliver D Doleski. *Herausforderung Utility 4.0.* Springer, 2017.

[22] Meike Löhr. "Grüne Umstellung, Energiewandel und Energiewende–Akteure in den Energiesystemtransformationsprozessen in Dänemark, Frankreich und Deutschland". In: *Energiewende.* Springer, 2018, pp. 79–129.

[23] European Commission Task Force for Smart Grids. *Expert Group 1: Functionalities of smart grids and smart meters.* 2010.

[24] Verband der Elektrotechnik Elektronik Informationstechnik e.V. *Die Deutsche Normungsroadmap E-Energy / Smart Grid.* `https://www.dke.de/resource/blob/2018912/3ae72fe24a471344af49c56d9ef36265/dke-normungsroadmap-1-ger-data.pdf`. 2010. (accessed: 04.2022).

[25] Claudia Eckert and Christoph Krauß. "Sicherheit im Smart Grid". In: *Datenschutz und Datensicherheit-DuD* 35.8 (2011), pp. 535–541.

[26] Edward A Lee. "Cyber-Physical Systems - Are Computing Foundations Adequate?" In: *Position paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap.* Vol. 2. Citeseer. 2006, pp. 1–9.

[27] Manfred Broy. "Cyber-physical Systems — Wissenschaftliche Herausforderungen bei der Entwicklung". In: *Cyber-Physical Systems.* Springer, 2010, pp. 17–31.

[28] Jairo Giraldo et al. "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys". In: *IEEE Design / Test* 34.4 (2017), pp. 7–17.

[29] Abdulmalik Humayed et al. "Cyber-Physical Systems Security—A Survey". In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831.

[30] Bartek Mika and Alexander Goudz. "Digitalisierung der Energiewende–Energiewende 2.0". In: *Blockchain-Technologie in der Energiewirtschaft*. Springer, 2020, pp. 25–36.

[31] Bundesamt für Sicherheit in der Informationstechnik. *Allgemeinverfügung zur Feststellung der technischen Möglichkeit zum Einbau intelligenter Messsysteme*. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/Marktanalysen/Allgemeinverfuegung_Feststellung_Einbau_01_2020.pdf?__blob=publicationFile&v=1`. (accessed: 09.2020).

[32] Bundesnetzagentur. *Smart Meter*. `https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Verbraucher/Metering/SmartMeter_node.html`. 2020. (accessed: 11.2020).

[33] Eric Ahlers, Yvonne Aniol, and Benjamin Scholz. "BDEW-Roadmap–Realistische Schritte zur Umsetzung von Smart Grids in Deutschland". In: *BDEW Bundesverband der Energieund Wasserwirtschaft eV, Tech. Rep* (2013).

[34] Deutscher Bundestag. *Gesetz über die Elektrizitäts-und Gasversorgung (Energiewirtschaftsgesetz-EnWG)*. Berlin, 2005.

[35] Deutscher Bundestag. *Gesetz zur Digitalisierung der Energiewende*. Berlin, 2016.

[36] Bundesamt für Sicherheit in der Informationstechnik. *Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*. Version 1.1. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf;jsessionid=ADE9FDDDC53E777A21B26062AEEDB484.internet462?__blob=publicationFile&v=4`. (accessed: 04.2022).

[37] Nils Hellmuth and Eva-Maria Jakobs. "Informiertheit und Datenschutz beim Smart Metering". In: *Zeitschrift für Energiewirtschaft* (2020), pp. 1–15.

[38] Michelle Goddard. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact". In: *International Journal of Market Research* 59.6 (2017), pp. 703–705.

[39] Alexandra Jorzig and Frank Sarangi. "Datenschutzgrundverordnung / Bundesdatenschutzgesetz". In: *Digitalisierung im Gesundheitswesen*. Springer, 2020, pp. 51–79.

[40] Bundesamt für Sicherheit in der Informationstechnik. *Das IT-Sicherheitsgesetz Kritische Infrastrukturen schützen*. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf;jsessionid=476CE34166CB225BB487DA13AA6552E2.internet461?__blob=publicationFile&v=1`. 2016. (accessed: 04.2022).

[41] Waldemar Grudzien. “IT-Sicherheitsgesetz–Gedanken zur Implementierung”. In: *Datenschutz und Datensicherheit-DuD* 40.1 (2016), pp. 29–33.

[42] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie BSI TR-03109-4. Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways.* Version 1.2.1. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-4_PKI.pdf?__blob=publicationFile&v=3%22`. (accessed: 09.2020).

[43] Bundesamt für Sicherheit in der Informationstechnik. *Digitale Gesellschaft. Smart Metering.* `https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/pki_node.html`. 2020. (accessed: 11.2020).

[44] Bayernwerk AG. *Abgeschlossene Regeleinsätze.*

[45] BDEW - Bundesverband der Energie- und Wasserwirtschaft e.V. *Smart Grids Ampelkonzept Ausgestaltung der gelben Phase.* URL: `https://www.bdew.de/media/documents/20150310_Smart-Grids-Ampelkonzept.pdf`. (accessed: 09.2020).

[46] Labor für Informationssicherheit und Compliance der Ostbayerischen Technischen Hochschule Regensburg. *Projektskizze Smart Energy Management Program - SEMP.* 2016.

[47] Labor für Informationssicherheit und Compliance der Ostbayerischen Technischen Hochschule Regensburg. *Projektskizze Secure Gateway Service for Ambient Assisted Living - SEGAL.* 2019.

[48] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz – Das Original in der Informationssicherheit.* URL: `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html`. (accessed: 09.2020).

[49] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 200-2 IT-Grundschutz-Methodik.* Version 1.0. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7%22`. (accessed: 09.2020).

[50] Heinrich Kersten et al. *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz.* Springer, 2008.

[51] International Standard. *ISO/IEC 29100:2011(E) Information technology — Security techniques — Privacy framework.* 2011.

[52] International Standard. *Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2016).* 2011.

[53] Andreas Prieß and Gabriela Hoppe. *Modellierung der Sicherheit von Informationssystemen mit DROPS.* Tech. rep. Diskussionsbeitrag, 2004.

[54] Paolo Bresciani et al. “Tropos: An Agent-Oriented Software Development Methodology”. In: *Autonomous Agents and Multi-Agent Systems* 8.3 (2004), pp. 203–236.

[55] Raimundas Matulevičius et al. “Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development”. In: *International Conference on Advanced Information Systems Engineering*. Springer. 2008, pp. 541–555.

[56] Wouter Depamelaere et al. “CPS Security Assessment Using Automatically generated Attack Trees”. In: *Proceedings of the 5th international symposium for ICS & SCADA cyber security research 2018*. British Computer Society (BCS). 2018.

[57] Neel A Patel et al. “4S Framework: A Practical CPS Design Security Assessment & Benchmarking Framework”. In: *Cyber Security and Digital Forensics* (2022), pp. 163–204.

[58] Wenbo Wu, Rui Kang, and Zi Li. “Risk assessment method for cyber security of cyber physical systems”. In: *2015 first international conference on reliability systems engineering (ICRSE)*. IEEE. 2015, pp. 1–5.

[59] Dmitry P Zegzhda, Maria A Poltavtseva, and Daria S Lavrova. “Systematization and security assessment of cyber-physical systems”. In: *Automatic control and computer sciences* 51.8 (2017), pp. 835–843.

[60] Ceeman Vellaithurai et al. “CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures”. In: *IEEE Transactions on Smart Grid* 6.2 (2014), pp. 566–575.

[61] Hamed Orojloo and Mohammad Abdollahi Azgomi. “A method for modeling and evaluation of the security of cyber-physical systems”. In: *2014 11th International ISC Conference on Information Security and Cryptology*. IEEE. 2014, pp. 131–136.

[62] Statistisches Bundesamt. *Mikrozensus 2019, Entwicklung der Privathaushalte bis 2040, Annahmen und Ergebnisse der 14. koordinierten Bevölkerungsvorausberechnung, Statistisches Jahrbuch*. 2019.

[63] Giorgio C. Buttazzo. “A General View”. In: *Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications*. Boston, MA: Springer US, 2011, pp. 1–22.

[64] K.G. Shin and P. Ramanathan. “Real-time computing: a new discipline of computer science and engineering”. In: *Proceedings of the IEEE* 82.1 (1994), pp. 6–24.

[65] Andreas Schilling. “Schutzmaßnahmen zur sicheren Identifizierung und Authentifizierung für Cloud-basierte Systeme”. In: *Identitätsmanagement im Cloud Computing*. Springer, 2018, pp. 33–51.

[66] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1: Vertrauensniveaus und Mechanismen*. Version 1.1.1. 2019. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf;jsessionid=38D0301AC6B1C9426B9414D30AE46768.1_cid501?__blob=publicationFile&v=4. (accessed: 09.2020).

[67] Jürgen Quade. *Harte und weiche Echtzeitsysteme.* 2004. URL: `https://ezs.kr.hsnr.de/download/20090921ezs.pdf`. (accessed: 09.2020).

[68] Michael Fiedler. *Grundlagen der Verschlüsselung und Authentifizierung (1): symmetrische Verschlüsselung und Authentifizierung.* 2010.

[69] Kjell J. Hole et al. "Risk Assessment of a National Security Infrastructure". In: *IEEE Security / Privacy* 7.1 (2009), pp. 34–41.

[70] Roland Bless et al. "Digitale Zertifikate, PKI und PMI". In: *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen* (2005), pp. 349–395.

[71] Radio Perlman. "An overview of PKI trust models". In: *IEEE network* 13.6 (1999), pp. 38–43.

[72] Joachim Swoboda et al. *Kryptographie und IT-Sicherheit.* Springer, 2008.

[73] Jens Bender and Dennis Kügler. "Was ist starke Authentisierung?" In: *Datenschutz und Datensicherheit-DuD* 40.4 (2016), pp. 212–216.

[74] Michael Kick. "Konzeption und Entwicklung eines Authentifizierungskonzeptes für Cyber-Physische Systeme im Anwendungsbereich Smart Grid". Bachelor Thesis. 2021.

[75] W.A. Janson. *A revised model for role-based access control.* NIST-IR 6192. National Institute of Standards and Technology, 1998.

[76] Berthold Heinrich, Petra Linke, and Michael Glöckler. "Grundlagen zur Automatisierung". In: *Grundlagen Automatisierung.* Springer, 2020, pp. 1–29.