Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT - 4-Level-Trust-Model as a Security Solution

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

Sebastian Fischer
Secure Systems Engineering
Fraunhofer AISEC
Berlin, Germany
email:
sebastian.fischer@aisec.fraunhofer.de

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

***Abstract*—The digital transformation has found its way into business and private life. It consists of digitization and digitalization. Digitization means the technical process and digitalization is the socio-technological process. Technologies of digitization are Cloud Computing (CC), Internet of Things (IoT) and Smart Grid (SG), which are separate technologies. The increasing digitalization in the private sector and of the energy industry connect these technologies. Actually, there is no connection between the CC infrastructure and the SG infrastructure at the moment, because in Germany the SG is currently under construction. If one looks at the CC and IoT, it must be stated there is an connection between the IoT infrastructure and the CC infrastructure as a service provider. To connect the technologies CC, IoT and SG and also build an SG cloud for innovative services, the new laws for privacy must be implemented. For privacy and security analyses it is important to know which data can be stored and distributed on a cloud. To illustrate this analysis, we connect the SG infrastructure with the IoT. An IoT device (car charging station) should be able to transfer data to and from the SG. SG is a critical infrastructure and the IoT device a potential insecure device and network. We show the communication between the smart meter switching box and the IoT device and the data transferred between their clouds. The charging station is connected to the SG to get the current amount of renewable energy in the grid. This is necessary to create a new smart service. But this service also generates private data (e.g., name, address, payment details). The private data should not be transferred to the IoT cloud. For the connection of SG and IoT, availability, confidentiality and integrity must be ensured. A risk analysis over all the cloud connections, including the vulnerability and the ability of an attacker, the resulting risk and the 4-Level-Trust-Model for security assessment are developed. Furthermore, we show the application of the 4-Level-Trust-Model in this paper.**

Keywords*—*Smart Grid; Internet of Things; security analysis; safety-critical infrastructure; cloud computing; 4-Level-Trust-Model

I. Introduction

This paper extends the already published paper "Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things" [1] with more detailed information of the risk analysis and the 4-Level-Trust-Model as a security solution for the main problem with the different data.

With the increasing digitalization in our world, new technologies, like the Internet of Things (IoT), have a great influence on our future way of life. Non-technical user are using connected technologies to improve their comfort without knowing about the possible risks.

But not only private technologies are increasing their digitalization, the future Smart Grid (SG) is also a highly networked system. In order to use these innovative services, which emerge from the digitalization, a third technology, Cloud Computing (CC) is necessary. With all three technologies combined, new services can be offered and the transformation of the energy system can be successfully implemented.

In Germany, the integration of the intelligent energy supply system (SG) is creating a new IT infrastructure. The intelligent measuring system (iMSys), containing a basic meter (smart meter) and the smart meter gateway (SMGW) [2] are currently installed in many households and companies in Germany. But other countries like Italy or Sweden are already further ahead with the development of the SG infrastructure.

The digitalization of the electricity grid brings new dangers and challenges in the area of IT-Safety and -Security. These can even allow attacks from the internet where no physical access to the network is necessary. Besides the SG, all kind of devices are getting a connection to the internet. These devices can range from smart refrigerators to connected cars and are called IoT. Most of the time, existing devices are getting a communication interface and are connected to the internet over a gateway or directly.

IoT, just like SG, also brings new IT-Security and -Safety dangers. For consumer devices, the damage is normally not high, but the lack of IT-Security in consumer devices, which are 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 necessary persistent. They are very flexible and appear and disappear quickly in their lifetime. This volatility is a big challenge for the security of existing and new services.

Beside of all dangers, new technologies are emerging and the new challenges must be solved. The smart services are required for future applications and the connection between

SG and IoT is necessary, to regulate the amount of energy in the grid. For these services, the cloud platform is needed as a connection between both technologies. It can be described as a data hub, for data storage, analysis and the services.

Both technologies, SG and IoT, are implementing their own cloud platform with the corresponding infrastructure. These independent clouds must be connected in order to offer new services with the desired added value. The potential insecure device and infrastructure of IoT should be able to communicate in both directions with the critical infrastructure of the SG. The security objectives availability, confidentiality, integrity and privacy must nevertheless still be ensured. Therefore, new risks and attack vectors emerge and new requirements for authentication and authorization are needed.

In this paper, we connect a IoT and SG cloud and perform a risk analysis over our example architecture to see the new problems and dangers of this connection. In the next step, a security model, based on IoT security standards and a new 4-Level-Trust-Model is developed. Finally, the model is applied to the example, to show the benefits of our security model.

The paper is structured as follows. Section II covers the related work and existing publications. In Section III, we describe our architecture and the corresponding challenges for the connection between the two technologies. In the next section, the security analysis is performed and Section V, describes the security model, which is applied in Section VI to our example. Finally, the conclusion is given.

II. Related Work

IoT devices are potential insecure devices. The security gaps in IoT devices can be protected with known principles. The problem is that they are not used by the manufacturers. One reason for this could be problem of costs. It is important for research to respond to new challenges in this field.

One challenge is the scarce resources of IoT devices. Already known encryption algorithms need to be adapted or changed to work more effectively and operate acceptably with low-performance hardware (e.g., PRINCE [3]). As an alternative, the new development of suitable algorithms can be considered (e.g., Secure IoT - SIT [4]).

Some publications cover the details about the necessary encryption and communication protocols, but do not classify the different data, e.g., [5] and [6]. The publication "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges" [7] describes an architecture for the combination CC and IoT, the "Cloud of Things". With the 4-Level-Trust-Model, a solution is developed to deal with the the mentioned security and privacy threats.

Currently, insecure devices are in use. For this situation, solutions must be found to continue the operation. The "Quad9 DNS Privacy and Security Service" is an example for this problem. Several companies (including IBM) have developed a special DNS server (Quad9 DNS Privacy and Security Service), which should ensure the security as well as privacy of the IoT devices. Quad9 automatically blocks requests to infected sites. As a last challenge, manufacturers must be "forced" to improve IT security. This can be accomplished by guidelines and certifications.

For SG exist an European architecture model so called Smart Grid Architecture Model (SGAM). This model was developed in the context of the European standardization mandate M/490. The SGAM includes the visualization, validation and structuring of SG projects from the beginning of the project as well as for the standardization of SG. The model was also used for the SG architecture development at different organizational levels. In this model, security is not explicitly considered. This publication describes security as a cross-cutting topic [8]. The architectural models of the countries differ in principle, but they are mostly based on the SGAM. In Germany, the SG itself is regulated by the specifications of the Federal Office for Information Security (BSI) and is regarded as the state of the art (communication) [9]. The BSI was commissioned by the legislator to develop specifications for a SMGW in order to guarantee a secure infrastructure for intelligent measuring systems [10]. The intelligent measuring systems will be integrated into a communication network with the central element SMGW as a communication unit [11]–[13].

Security and privacy considerations for IoT application on SG with a focus on survey and research challenges presented are shown in [14] and [15]. The publication gives a brief insight SG and IoT application on SG. Furthermore, the publication identifies some of the remaining challenges and vulnerabilities related to security and privacy. A security and communication analysis of SG, IoT and CC in Germany are shown in [16]–[18]

Classical models for IT security assessment are the BSI-Standards (BSI-Standards 200-1, 200-2 and 200-3 [19]–[21]) or ISO/IEC 27000:2018 [22], which classically consider the IT processes within a company. With highly scalable and distributed systems (such as CC, IoT and SG), the entire IT process must be considered. In [23]–[26] security is considered during the development process of software. The security evaluation of data is based on a 2-level trust model shown in [27]. These known models for security modeling as well as the 2-level trust model are not suitable for cyber physical systems (CPS).

The handling of data when they leave the "SG", requirements for authentication and authorisation in future SG-IoT-cloud application and how to deal with service provider who access data (service charging station) in critical infrastructures are open questions. For this open question there is no related work.

III. Architecture Challenges for Smart Grid and IoT

First, we describe the challenges in SG and IoT individually, then we present our example architecture with the communication and the corresponding data.

TABLE I. 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

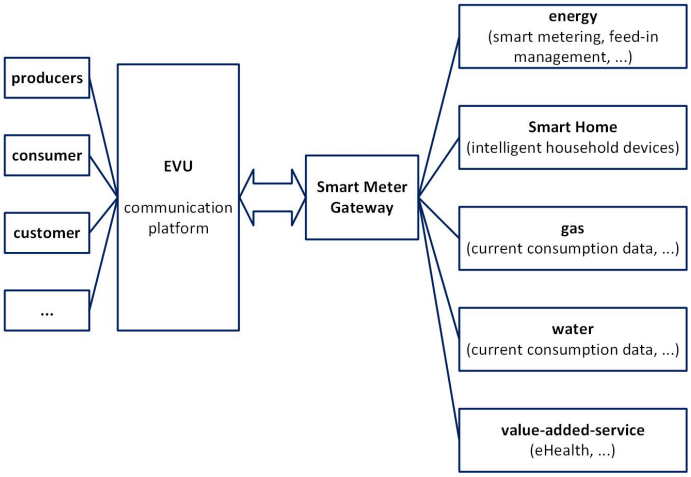

Figure 1. Application example Smart Grid

A. Smart Grid

In the future SG (compare Table I), large amounts of data are generated daily when meter data are read out on a regular basis. These data have to be stored, archived and analyzed. The conversion of the entire energy supply system from a centralized supply to a decentralized supply is progressing continuously in Germany [28]. The transformation of the energy supply to an intelligent energy supply system creates numerous new opportunities and challenges. The changeover to renewable energies alone, such as wind power or solar energy, creates new challenges for future systems in the SG.

The SG infrastructure is not only used for the use case "energy" like smart metering (see Figure 1). Further filed of application are smart home, gas, water and value-added service. The energy supplier (EVU) operates a data platform to connect the users. In this case, user are producer, consumer and customer. The SMGW is the secure interface and communication unit between the household and the EVU.

The conversion is not only taking place in Germany, but also in other European countries. Pioneers are countries like Italy and Sweden [28]. However, these rollouts have already been carried out the dangers from a security and safety perspective. With regard to security of supply, attacks on control systems of the power grid via the Internet represent a growing threat, because on the one hand, the power grid can be controlled or manipulated over it. On the other hand, data requiring protection about the consumer and their behaviour can be accessed. This is because data of varying origin and quality is processed and analysed in real time. As a result, access to the systems must be guaranteed for different groups of people.

B. Internet of Things

The Internet of Things is defined in the ISO/IEC 20924:2018 standard as a infrastructure, which connects entities with services which react to information from the physical and virtual world [29]. This includes all connected devices nowadays, regardless if they are connected to the Internet or not. In our paper, we restrict this definition to common IoT devices, which benefit from a connection with the SG. This mainly includes smart home devices with a high energy consumption like a smart charging station.

Especially smart home devices are currently highly insecure, because of the increasing amount of devices [30] and the cheap price. Nearly every home appliance devices needs a connection to some smartphone application and the internet to control them remotely. This leads to a fast development of new features and connection points without enough time to care about the security. The second security issue is price, because no customer is willing to pay more for a device just because it was designed to be secure. The cheapest device with the most features is usually always bought.

Botnets like Mirai [31] and other malware are using insecure IoT devices, to attack other networks. The security problems of IoT are not new and the majority of them can be solved with common IT-Security methods. This shows the OWASP IoT Project. The top vulnerabilities in IoT devices, like default or weak passwords, are simple to fix [32].

Because of this, we consider IoT devices as insecure. There are too much insecure devices in operation and there is no prove of security of new devices. Nevertheless, we connect an insecure IoT network to a probably insecure cloud and this cloud finally to the SG.

C. Architecture Smart Grid and IoT

The SG reference architecture consist of the Local Metrological Network (LMN), the Wide Area Network (WAN) and the Home Area Network (HAN). The connection between these networks takes place through the SMGW. The LMN consists of all the gas meter, electricity meter, etc. The WAN is outside of the building and describes the connection over a wider range. The Gateway-Administrator and the energy supplier (Energieversorgungsunternehmen in German, short EVU) are located in the WAN. The last network, the HAN, is the local network in the building with the connected (smart home) devices. The SG cloud extends the common SG reference architecture, as shown in Figure 2.

The IoT network is located in the HAN with all connected IoT devices. Some devices are connected over a gateway to the Internet. The IoT Cloud and the user can access theses devices over these HAN connections.

New services can use the central stored data of the cloud platforms and make it available to the user. As shown in Figure 2, the connection between IoT and SG can be established

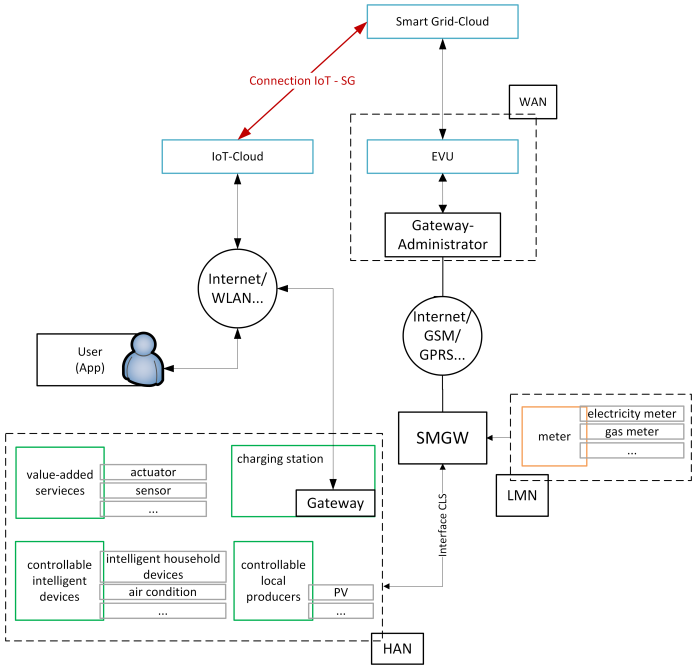

Figure 2. Architecture Cloud Application on Smart Grid with IoT

between the two clouds (IoT Cloud and SG Cloud). It is the main focus of this paper, as this is where the two technologies are combined and data exchange takes place.

D. Application Example

For a realistic and useful example, we use a smart car charging station with a cloud connection. The charging station is considered as insecure, as well as the whole IoT network (Gateway, Cloud, Applications). The SG network is as extensive as described in the previous section with all the components. As meter, a electrical meter is used, because the smart service should connect the charging station cloud and the SG cloud. The service can load the electric car, connected to the charging station, at the most suitable times. The grid can charge the car, when a lot of energy is produced and therefore in the grid. If the grid is low on energy (can be detected by the current frequency), the car can supply the grid with stored energy to stabilize it. The smart service connects the two clouds, because at this point it is possible to get all necessary data from both technologies.

E. Communication between Smart Grid and IoT

By connecting the two clouds, data is exchanged. To determine the risk of the connection, it is necessary to know which data is transferred. There are only the communication data from IoT and SG listed, because not all stored data is exchanged.

1) Communications data Internet of Thing: The following data is stored in the IoT cloud and transmitted to the smart service as needed:

- ID Connected car
- ID gateway (charging station (CS))
- IP-Address gateway (CS)
- Sum of energy consumption (CS)
- Current energy consumption / supply (CS)
- History of energy consumption / supply (CS)
- Time to load the car
- User data (CS)
  - Name
  - E-Mail

The connected car and the history can be used to create a profile of the user. This includes the times, the user is normally at home or at work. This data is private data and should be protected.

2) Communications data Smart Grid: The following data is generated and stored in the SG cloud, as well as transmitted to the smart service:

- Information about the smart meter (ID, IP-Address)
- Current energy consumption
- Current price for electricity
- Information about the customer
  - Name
  - Address
  - Payment details

The information about the smart meter or the current energy consumption can be used to create a profile of the household (user). This is partly equal to the profile of the connected car, but can be extended to the whole household an therefore other people. In conclusion, like the connected car data, this data is also private data and should be protected. Special data protection precautions must be taken, as this may allow conclusions to be drawn about third parties (other people in the household).

IV. Security Analysis for Safety-Critical Systems

The security analysis starts with the description of the attack vectors. From these vectors, the threads are derived. In the next step, the risk is shown for every thread, based on the ability of the attacker and the possible damage. Finally, practical examples show the potential danger in our example architecture.

A. Attack vector Smart Grid and Internet of Thing

There are four kind of attack vector categories: hardware manipulation attacks (physical attacks), software manipulation attacks, network-based attacks and privacy related attacks [33] [34]. Each attack tries to get unauthorized access to the infrastructure or inflict some damage to it [35].

Hardware manipulation or physical attacks are performed locally on the device. It is possible to change the hardware and the software. Mostly malware is installed, which leads to data manipulation and sniffing. In context SG, a complete shutdown of the grid would be possible in the worst case. However, sensitive (private) data can also be tapped and modified. In

the case of IoT devices, for example, the software can be modified so that the device acts as a spy and forwards all data to the attacker. Hardware attacks thus open up all possibilities for an attacker, but are very difficult to execute.

With software manipulation attacks, it is possible to change the software (or firmware) of the device. These attacks can be done remotely over the internet or any other network. The attacker uses a weakness in the running software (e.g., buffer overflow, code injection) to execute his own code or tries to manipulate the administrator of the device to install the malicious software. As with hardware manipulation attacks, in the worst case the SG can be shut down or sensitive (private) data can be modified or tapped.

Network-based attacks like identity theft, denial of service, cascading malware propagation (Business IT & Plant Control) and monitor, traffic analysis (passive attacks) are using the network to inflict damage. They can be used to get data or to disable the service. These attacks are difficult to protect from, because the hole network (internet) is not controlled.

The last category are privacy related attacks. With these attacks, user-specific data are collected and used to inflict personal damage to the customers or the energy supplier. They can be combined with other attacks or used to trick the administrator to install malicious software (social engineering).

According to IoT and SG, the following risks are possible: manipulation of measured values and time, manipulation of the communication between IoT cloud and SG cloud, misuse of energy data and/or sensitive data, sabotage of the power grid and sabotage of mobility (example: charging station).

B. Security threats: Infrastructure Smart Grid and Internet of Things

The risk analysis for both, the IoT cloud and the SG cloud, are including the ability of an attacker and the potential damage, which are leading to a risk for the associated attack. With a lower ability, it is more likely for an attacker, to use this kind of attack [36]. The potential damage of an attack is related to the real damage (destroy some parts of the grid or the unavailability of services) and the personal damage, caused by stolen private information. For example, an attacker gets private data from the SG, the ability needs to be high, but the damage is high, too. This lead to a high risk overall [37].

Because of strict specifications and regulations of the SG in Germany, the ability of an attacker must be high in the most cases.

1) DoS and DDoS: A (distributed) denial of service (DDoS or DoS) attack tries to flood the device or network with too much data, so the service becomes unavailable. This kind of attack can be performed distributed with a lot devices from a botnet at low costs.

For IoT devices there is low damage, because most of them are just for comfort features. Necessary devices, like electric cars, are not available in high amounts at the moment, so not many of them are affected. For the SG, such an attack can lead to a shutdown of the grid, because the SG is unable to broadcast the current amount of energy in the grind and all connected cars start charging. The medium and high damage, combined with the low ability needed, are leading to medium to high risks for both technologies.

Ability of an attacker
IoT: low SG: low
Damage
IoT: medium SG: high
Risk
IoT: medium SG: medium / high

2) Malware: For using a malware, the attacker needs to know or find a vulnerability in the software. This can be very easy in IoT devices, because of the bad security situation. For eamxple, the mirai botnet started by using easily guessable login credentials to compromise the devices [31].

The SG is strictly regulated in Germany by the Federal Office for Information Security with the technical regulations TR-03109 [8]. This certification is needed to operate the devices, so they can be declared as secure and the ability of an attacker has to be high to attack them.

The damage for IoT is similar to the one for the DoS and DDoS attacks. But the SG can be compromised and the attacker can shutdown the hole grid or even damage hardware components.

The derived risk of a malware attack is therefore medium for IoT and medium to high for SG.

Ability of an attacker
IoT: low SG: high
Damage
IoT: medium SG: high
Risk
IoT: medium SG: medium / high

3) Broken Authentication: Like shown at malware attacks above, the broken authentication is very similar. The IoT devices are not secure and the SG is considered as secure, because of the certification.

The damage and the risk were also assessed as in the malware section. A broken authentication can lead to a full compromisation of the device or the network.

Ability of an attacker
IoT: low SG: high
Damage
IoT: medium SG: high
Risk
IoT: medium SG: medium / high

4) Broken Encryption: The broken encryption is also very similar to the malware attacks. The IoT devices are not secure and the SG is considered as secure, again because of the certification.

The damage is not so high as malware or broken authentication, because only the data send over the network can be attacked. Depending on the content of the data, personal information may be included, but the confidentiality of the

data is not necessary for the operation. The damage at IoT can be low to medium, because of the different device types. The SG can expose more personal information, so the damage is medium.

Because of the low ability and the low to medium damage, the risk of IoT is medium. In the SG a high ability is needed, which leads to medium damage, the risk is declared as medium.

Ability of an attacker
IoT: low SG: high
Damage
IoT: low / medium SG: medium
Risk
IoT: medium SG: medium

5) Data leakage: When a part of the data or all data are exposed, the damage and the risks are the same as by broken encryption. The ability is also rated the same, but can be a bit lower, because sometimes no encryption at all is used for IoT devices.

Ability of an attacker
IoT: low SG: high
Damage
IoT: low / medium SG: medium
Risk
IoT: medium SG: medium

6) Data manipulation: As mentioned before, data manipulation can be easily performed in IoT environments, because of missing regulations. For example, the IoT Cloud can be attacked and adopted, because easy to guess passwords are used. As the last sections, the SG network is secure and no data can be manipulated.

In the most cases, the manipulation of data for IoT devices is only possible for one kind of device or one manufacturer. This limits the damage and therefore has no great effect on the SG. If SG data are manipulated, it can lead to some damage, but not for all user, just for the affected ones. Therefore, the damage for IoT is low and for SG medium.

The risk was assessed as before. A low ability and a low damage are leading to a low risk. A high ability and a medium damage to a medium risk.

Ability of an attacker
IoT: low SG: high
Damage
IoT: low SG: medium
Risk
IoT: low SG: medium

7) Hardware manipulation: It is very difficult to get access to the hardware. The cloud server are most of the times under good protection, especially in the SG and the devices are installed in the house. If an attacker gets access to one house, it is only one device affected and not the whole network. These points are leading to a medium and a high ability for the attacker.

If it is possible to get hardware access to the cloud, the damage can be medium to high. For an IoT device, the attacker only gets access to one or some manufacturer. But the SG cloud can be used to shutdown the whole grid.

The risk is straight forward for IoT, because the ability and the damage are both medium. For the SG, the risk is medium because it is difficult to attack the server infrastructure.

Ability of an attacker
IoT: medium SG: high
Damage
IoT: medium SG: high
Risk
IoT: medium SG: medium

	IoT risk	SG risk
DoS und DDoS	medium	medium / high
Malware	medium	medium / high
Broken Authentication	medium	medium / high
Broken Encryption	medium	medium
Data leakage	medium	medium
Data manipulation	low	medium
Hardware manipulation	medium	medium

Figure 3. Summary of the risks

C. Summary of the security analysis

As shown in Figure 3, the summary of the risks shows that the SG is always exposed to at least medium risk (sometimes medium to high), while for IoT, the maximum is medium. This shows a need for action, especially for SG.

D. Examples

In the following, we show a few examples of how the problems by connecting IoT and SG can be recognized. The first two examples are from [1]. As an IoT device and the according infrastructure are currently highly insecure [38], all problems are realistic and the data from IoT can be considered easily accessible.

Example 1: The user can register his IoT device in the IoT cloud only with a valid E-Mail address and a username. No further information is needed. The IoT provider only knows that this username has loaded his car 20 times per month. By exchanging data with the smart meter, detailed information(name, address) about the user can be transferred. Now it is possible to identify the user.

Example 2: The energy service provider does not need any information of the connected car of the user. But with additional information from the IoT charging station, it is possible to tell when the user is at home or if he gets visited by another person with an electric car. This part is very important. A third user can be tracked with his car, without knowing it.

Example 3: The SG customer does not wish to disclose any personal information about his purchasing behaviour or financial situation. If, however, data of the car (cheap or expensive

car) and the charging points (e.g., at which supermarket the car is charged) are exchanged, an exact profile of the user can be created with the additional personal information from the SG.

Example 4: A hacked charging station can be made by software to charge at times when the electricity price is high. This can also result in financial damage for the user.

All four examples are showing the importance of a security and privacy orientated connection. As default no data should be transferred between the clouds. The user should have to confirm each data exchange.

V. Security model

We are presenting two parts, to improve the security of our example. The first part consists of security standards for IoT, which are currently under development and the second part shows a 4-Level-Trust-Model. The security standards are just a overview, but the 4-Level-Trust-Model is a development by our own.

A. IoT Security Standards

In order to increase the security of IoT devices, security and privacy must be taken into account during the development phase (Security- and Privacy-by-Default). Since most manufacturers are currently foregoing such measures because of the costs, guidelines and standards must be developed to implement a minimum level of security.

In Germany, DIN SPEC 27072 was published in 2019 [39], which sets minimum security requirements for consumer devices. These include a secure password, encryption, updates, etc. This standard is currently not mandatory and manufacturers of IoT devices can voluntarily develop their products according to it.

In 2020, the UK Government has published a guideline, which is also aimed at consumer devices and will be binding. It focuses on three aspects [40]:

- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers of IoT products explicitly state the minimum length of time for which the device will receive security updates.

Besides these local standards, the European Telecommunications Standards Institute (ETSI) is working on EN 303 645 - Cyber Security for Consumer Internet of Things. This standard is currently available as a draft and has similar requirements according to the DIN standard. The main focus are also consumer devices, but with less restrictions.

The current EN 303 645 draft consists of requirements, grouped into the following thirteen topics [41]:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is protected
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

TABLE II. New ability of an attacker and new risk by applying standards

	ability	ability new	risk	risk new
DoS und DDoS	low	low	medium	medium
Malware	low	medium	medium	medium
Broken Authentication	low	high	medium	medium
Broken Encryption	low	high	medium	low
Data leakage	low	medium	medium	low
Data manipulation	low	medium	low	low
Hardware manipulation	medium	medium	medium	medium

In the future, when IoT devices will be developed with the help of security standards, the risk analysis will no longer have to assume that the attacker needs little effort to attack the device and the risk will be significantly reduced. Furthermore, for most use cases, considerably less personal information can be collected and stored, making it more difficult to obtain sensitive information. For example, a networked refrigerator does not have to identify its user exactly (with name, address, etc.). Authentication without further user details or a social media account is sufficient.

The risk analysis for IoT changes with the improvements of the standards. The requirements about passwords, updates, encryption, authentication and data minimization are leading to higher abilities and therefore to a lower risk. The new values for the ability of an attacker and the risk can be seen in Table II. These new values are just assumptions, because some requirements are not mandatory and can improve the security even more, depending on whether they are implemented.

B. 4-Level-Trust-Model for safety-critical systems

Data are to be regarded as endangered property. The 4-level trust model is intended to protect the data (depending on its specification). For example, all smart meter data are data worthy of protection [42]. This is a statement of the state conference of data protection officers. It means that all data (IP adress, frequency, customer data, etc.) must be specially treated during processing, transmitting and storing. Data generator and user are human and machine also. The processing of data is in real-time not now but in future. SG is a variant of CPS. The requirements of future Systems like SG are:

- High scalable:
  The use case data logging electricity shows us the Data flaw from final consumers to the energy supplier. This

means 2 million participants and 192 million consumption values per day.
- Volatile:
  If we have a look inside the communication. There are data transfer every 15 minutes.
- High data volume:
  For example, 2 million households generating 22 gigabyte data per day.
- Different types of data:
  Customer data, power consumption, IP address, etc.

Security assessment must be adapted with regard to these additional requirements. The 4-Level-Trust-Model for safety-critical systems was developed based on the requirements. The 4-Level-Trust-Model for safety-critical systems is one option of the role-based trust model for safety-critical systems [43]. This is a model for security assessment for CPS. Classically, data are divided into two categories - secure and insecure. This is described as the classical security model. In the new 4-Level-Trust-Model for safety-critical systems the data are categorized in 4 categories. The categorization depends on the requirements analysis for CPS. The 4-Level-Trust-Model for safety-critical systems is defined as follows.

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

Table III shows the 4-Level-Trust-Model for safety-critical systems with the coding and the security level. The 4-Level-Trust-Model for safety-critical systems permits to consider the security assessment of data.

TABLE III. Evaluation criteria data security

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

With the 4-Level-Trust-Model it is possible to evaluate data and information of a use case in CPS with regard to security. By subdividing the data worthy of protection, a further gradation between personal data and sensitive data is made. With this model, appropriate security measures can be selected. The security measures for SG must be taken from the respective standards of the BSI. Security measures for IoT must be taken from the corresponding standards (see above).

The proposed model is an extension of the 3-Level-Model (such as security evaluation according to the BSI standards) and is a possibility to perform security evaluation in CSP. The 4-level model has proven itself in application.

VI. Application example: 4-Level-Trust-Model for safety-critical system

In the following section, we present the security assessment based on the 4-Level-Trust-Model for safety-critical systems. The application example is SG and IoT: charging station (see Section III, part D). Table IV shows the security assessment in detail. We categorized the data and matched the security level.

For example, the “ID connected car” is a data type for the third category. The security level is “intermediate” and the coding is “2”. In combination with one data of the second category is an personal reference possible. Another example is the assessment of the history of energy consumption / supply CS. This is a data type for the second category. The security level is “minimal” and the coding is “1”. In combination with several data (e.g., ID Gateway CS, IP-address) of the third category is an personal reference possible. For example, the information about the customer are a data type from the fourth category. The security level is “high” and the coding is “3”. The data are personal data like name or street.

This security analysis enables the selection of appropriate security measures (e.g., authentication). For the authentication of devices which transmit data such as ID Gateway CS (category 3), a procedure that guarantees a high level of security can be selected. On the other hand, a minimum level of security can be ensured for the authentication of devices that transmit data assigned to the category 2 (e.g., history of energy consumption / supply CS).

TABLE IV. Evaluation of the data security: use case charging station (SG and IoT)

data	category	security level	coding
ID connected car	3. Category	intermediate	2
IP-Address Gateway (CS)	3. Category	intermediate	2
ID Gateway (CS)	3. Category	intermediate	2
IP-Address smart meter	3. Category	intermediate	2
IP-Address smart meter	3. Category	intermediate	2
Sum of energy consumption CS	2. Category	minimal	1
Current energy consumption / supply CS	2. Category	minimal	1
History of energy consumption / supply CS	2. Category	minimal	1
Time to load the car	2. Category	minimal	1
User data CS	4. Category	high	3
smart meter ID	3. Category	intermediate	2
IP-Address smart meter	3. Category	intermediate	2
SMGW ID	3. Category	intermediate	2
IP-Address SMGW	3. Category	intermediate	2
Current energy consumption (SG) smart meter ID	2. Category	minimal	1
IP-Address smart meter	3. Category	intermediate	2
Current price for electricity smart meter ID	2. Category	minimal	1
IP-Address smart meter	3. Category	intermediate	2
smart meter ID	3. Category	intermediate	2
IP-Address smart meter	3. Category	intermediate	2
Information about the customer	4. Category	high	3
IP-Address smart meter	3. Category	intermediate	2

VII. Conclusion

In this paper, we show different challenges for the digitization and digitalization. New connected technologies, like the SG and IoT are getting connected. This can result in some serious security issues, because the SG is a critical infrastructure and current IoT devices are insecure. In our application example, a car charging station with its corresponding cloud (IoT) is connected to the SG infrastructure. For this use case example, we carried out a security analysis for safty-critical infrastructures. We show the attack vectors of SG an IoT and the security threats. The SG is always exposed to at least medium risk (sometimes medium to high), while for IoT, the maximum is medium. Due to these high risks, security by connecting the two technologies must be significantly improved. Four examples were presented of why lack of security is a problem.

For improvement, IoT devices can be secured by applying standards, like the DIN 27072 or the European version from ETSI - EN 303 645. As an advanced solution, we introduced the 4-Level-Trust-Model for safety-critical systems. The 4-Level-Trust-Model is one option of role-based trust model. With this model, data and information of a system can be evaluated. A distinction is made between personal data and sensitive data. With this security assessment, CPS can be evaluated. This model offers assistance in the selection of appropriate security measures. We have shown the application of the 4-Level-Trust-Model using the application example "connect a charging station with a cloud to SG infrastructure".

The security standards and our trust model can only help to decrease the risks. To establish a highly secure connection between IoT and SG, more considerations are needed. The interfaces must be clearly defined and communication must be restricted accordingly. A detailed risk analysis on the concrete architecture is as necessary as extensive penetration tests.

The 4-Level-Trust-Model provides a good basis and the next step is to implement the model to demonstrate its functionality in practice. It will be some time before the two technologies (IoT and SG) are connected in Germany and by then, a complete secure infrastructure model can be developed.

References

[1] K. Neubauer, S. Fischer, and R. Hackenberg, Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 82-87, 2019.

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

[3] H. Kim and K. Kim, Toward an Inverse-free Lightweight Encryption Scheme for IoT, Conference on Information Security and Cryptography, 2014.

[4] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, CoRR abs/1704.08688, 2017.

[5] I. Ben Dhaou, A. Kondoro, A. Kelati, D. S. Rwegasira, S. Naiman, N. H. Mvungi, and H. Tenhunen, Communication and Security Technologies for Smart Grid, International Journal of Embedded and Real-Time Communication Systems (IJERTCS), 8(2), pp. 40-65, 2017.

[6] D. G. Korzun, I. Nikolaevskiy, and A. Gurtov, Service Intelligence and Communication Security for Ambient Assisted Living, International Journal of Embedded and Real-Time Communication Systems (IJERTCS), 6(1), pp. 76-100, 2015.

[7] A. A. A. Ari, O. K. Ngangmo, C. Titouna, O. Thiare, A. Mohamadou, and A. M. Gueroui, Enabling Privacy and Security in Cloud of Things: architecture, applications, security & privacy challenges, Applied Computing and Informatics, 2019.

[8] M. Uslar, C. Rosinger, and S. Schlegel, Application of the NISTIR 7628 for Information Security in the Smart Grid Architecture Model (SGAM), VDE Kongress, 2014.

[9] Bundesamt fuer Sicherheit in der Informationstechnik, Technische Richtlinie, BSI TR-03109, 2015.

[10] P. Peters and N. Mohr, Digitalisierung im Energiemarkt: Neue Chancen, neue Herausforderungen, Energiewirtschaftliche Tagesfragen, pp. 8-12, 2015.

[11] V. C. Gungor et al., A Survey on Smart Grid Potential Applications and Communication Requirements, IEEE Trans. Ind. Inf. 9 (1), pp. 28-42, 2013.

[12] X. Li et al., Securing smart grid. Cyber attacks, countermeasures, and challenges, IEEE Commun. Mag. 50 (8), pp. 38-45, 2012.

[13] C. Wietfeld, C. Muller, J. Schmutzler, S. Fries, and A. Heidenreich, ICT Reference Architecture Design Based on Requirements for Future Energy Marketplaces, 1st IEEE International Conference on Smart Grid Communications, pp. 315-320, 2010.

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

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

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

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

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

[19] Bundesamt fuer Sicherheit in der Informationstechnik, BSI-Standard 100-1 Managementsysteme fuer Informationssicherheit (ISMS), 2008, [Online]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile&v=2 [retrieved: 02, 2020].

[20] Bundesamt fuer Sicherheit in der Informationstechnik, BSI-Standard 200-2 IT-Grundschutz Methodology, 2017. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=1 [retrieved: 02, 2020].

[21] Bundesamt fuer Sicherheit in der Informationstechnik, BSI Standard 200-3: Risk Analysis based on IT Grundschutz, 2017. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2 [retrieved: 02, 2020].

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

[23] R. Matuleviius, N. Mayer, H. Mouratidis, E. Dubois, P. Heymans, and N. Genon, Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development, International Conference on Advanced Information Systems Engineering, pp. 541-555, 2008.

[24] P. Bresciani et al., Tropos: An Agent-Oriented Software Development Methodology, Autonomous Agents and Multi-Agent Systems 8, pp. 203236, 2004.

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

[26] L. Compagna et al, How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns, Artif Intell Law 17, pp. 130, 2008.

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

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

[29] International Organization for Standardization, ISO/IEC 20924:2018 Information technology - Internet of Things (IoT) - Vocabulary, 2018.

[30] Heise Medien, Wachsende Bedrohung durch unautorisierte IoT-Geraete, 2020. [Online]. Available from: https://www.heise.de/ix/meldung/Wachsende-Bedrohung-durch-unautorisierte-IoT-Geraete-4668472.html [retrieved: 02, 2020]

[31] B. Herzberg, I. Zeifman, and D.Bekerman, Breaking Down Mirai: An IoT DDoS Botnet Analysis, 2016. [Online]. Available from: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet [retrieved: 01, 2020].

[32] The OWASP Foundation, OWASP Internet of Things, 2018. [Online]. Available from: https://owasp.org/www-project-internet-of-things/ [retrieved: 02, 2020].

[33] R. Sichler, Smart und sicher geht das?, Springer Fachmedien Wiesbaden, pp. 463-494, 2014.

[34] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, Proposed embedded security framework for Internet of Things (IoT), Electronic Systems Technology (Wireless VITAE), 2010.

[35] C. Eckert, IT-Sicherheit, Konzepte - Verfahren - Protokolle, Boston De Gruyter, 2012.

[36] L. ben Othmane, H. Weffers, and M. Klabbers, Using Attacker Capabilities and Motivations in Estimating Security Risk, Symposium On Usable Privacy and Security, 2013.

[37] The OWASP Foundation, OWASP Risk Rating Methodology, 2019.

[38] The OWASP Foundation, Internet of Things Project, IoT Vulnerabilities, 2019.

[39] Deutsches Institut fuer Normung, DIN SPEC 27072: Informationstechnik - IoT-fhige Gerte - Mindestanforderungen zur Informationssicherheit, pp. 1-16, 2019.

[40] United Kingdom Department for Digital, Culture, Media & Sport, Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation, 2020.

[41] European Telecommunications Standards Institute, Draft ETSI EN 303 645 V2.0.0, pp. 1-30, 2019.

[42] Konferenz der Datenschutzbeauftragten des Bundes und der Lnder und Dsseldorfer Kreis, Orientierungshilfe datenschutzgerechtes Smart Metering, 2012. [Online]. Available from: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_smartmeter.pdf [retrieved: 02, 2020].

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