Current State of the Art in Smart Metering Security

SICS Technical Report T2015:03

Rikard Höglund
SICS Swedish ICT AB, Security Lab
Isafjordsgatan 22, Kista, Sweden
Email: rhoglund@sics.se

Marco Tiloca
SICS Swedish ICT AB, Security Lab
Isafjordsgatan 22, Kista, Sweden
Email: marco@sics.se

April 30, 2015

Abstract

Power supply infrastructures are facing radical changes. The introduction of Information and Communication Technologies (ICT) into power grids will allow to automatically monitor and control the power demand and supply. This concept is generally referred to as Smart Grid, and is expected to exponentially grow during the coming years. However, ICT systems are increasingly subject to security cyber attacks, which can have a disruptive impact on the whole power grid, and put people's safety and business interests at risk. This report covers background information on the smart grid with focus on smart metering in particular. Important aspects such as security and life-cycle management are covered. In addition, the typical smart grid components and communication protocols are surveyed.

Index

1. Introduction

Historically, power grids have been composed of few large components with the main function to distribute power and dispatch control commands in a single direction, namely towards end devices. That is, this classical grid is in general asymmetric in terms of communication. Some components can provide control functionalities, but this is usually limited to the core of the grid, and not implemented on a single component basis. The need for monitoring the grid has emerged quite fast, as gathering information is important to maintain stability and safety. In fact, a power grid can be sensitive to fluctuations in power loads, and it is possibly for localized faults to easily escalate and spread quickly, so causing wider and more severe effects. Therefore, it is vital to promptly address unpredicted circumstances, issues and maintenance needs. This is the reason why adding intelligence and monitoring capability to power grids has been a gradual but fast process, which could massively benefit from the rapid development in IT areas.

Smart grid is a class of technology that modernizes electricity delivery systems by using computer-based remote control and automation [45]. In particular, the introduction of Information and Communication Technologies (ICT) into power grids allows automatic monitoring and control of the power demand and supply. Practically, a smart grid relies on remotely controlled actuators and switches for controlling the grid, and sensors and meters that continuously monitor the current power flow and other important statistics. Getting such accurate information results in a number of benefits. They include ensuring quick reactions in case of faults or malfunctioning, automatically detecting and locating faults to promptly dispatch repair teams, performing load-balancing of the network and implementing pro-active strategies to maintain the stability of the grid.

A *smart meter* is a particularly important component in smart grids, and is supposed to be deployed especially in individual customers' homes. In particular, such devices allow the collection of accurate power metering data from all customers of a given energy operator. In addition, the energy operator can remotely send commands to smart meters in order to trigger different actions on the customers' side. For instance, it can be asked to reduce the current power usage or to interact with private home appliances, e.g. to selectively control them. At the same time, there are also a number of benefits for the customer. For instance, he can be informed about preferable consumption patterns, which would result in reducing the energy bill. Furthermore, it becomes easier to manage private production of power, such as through solar cells, and sell it to the energy operator. Finally, providing customers with accurate statistics about their own power usage can further help to reduce power consumption and related costs.

Security is particularly important in a smart grid architecture. Since ICT systems are increasingly subject to security attacks, smart grids inevitably inherit a number of security threats and vulnerabilities, at the network, application and platform level. Besides, possible unauthorized physical accesses to smart grid components may allow retrieval of sensitive data and security material. Even the final customer can be motivated to tamper with the smart meter at his own private residence, in order to defraud the billing process. In general, a successful attack against a smart power grid can result in severe, possibly large scale, consequences. For instance, gaining access to the control system components makes it possible to increase the power load on certain parts of the grid, or damaging transformer stations. This is only one of many possible attacks, whose effects on society can be devastating in terms of people's safety and business interests. Loss of power in an area can affect hospitals, impact on food storage facilities and services, and cause countless secondary accidents due to the lack of power. A single software bug, along with other concurring factors, caused overloading in several parts of the network and created a large blackout affecting up to 55 million people in the northeast United States during 2003 [44].

This document overviews important components and security aspects related to smart grids, with particular focus on the smart metering process and smart meter devices. The goal is to give a broad picture of the current state of the art with reference to different relevant areas. Currently, there are several documents focusing on single aspects such as communication protocols or management of cryptographic material. Instead, it is more difficult to find a single resource that gives a more complete picture of multiple security issues related to smart grids and smart metering.

The rest of this document is organized as follows. Chapter 2 provides an overview of the smart grid concept. This includes the historical development of power grids, the emergence of smart grids and what benefits they provide. Chapter 3 covers platform security for smart meters. Relevant topics on this area are hardware, software and virtualization solutions. Chapter 4 discusses life-cycle management in smart grids. Key management and initial provisioning of keys are two particular aspects covered. Chapter 5 presents different communications protocols that are commonly used in smart grids. Since the grid can be separated into different communications levels, there are also protocols that are suitable for each level. For instance, communication between smart meters and home appliances relies on some communications protocols, while different ones are used in other portions of the grid. Finally, Chapter 6 focuses on security in smart grids, and overviews some threats and possible solutions.

2. Overview and Background

This chapter describes the background and historical development of the power grid and smart grid. The first section goes through some of the history of the traditional power grid and how it has developed. This includes the structure of the classical power grid and how the monitoring came to be needed. It also mentions some of the historical development and improvements to the power grid. The second section considers the improvements that the smart grid provides. Both customer and producer can benefit in a number of ways from the functionality the smart grid provides. The same section also considers why security is an important challenge for smart grids and why an attack against the power grid can have significant negative effects.

Traditional power grids are yesterday typically composed of a few but large power stations connected with high-capacity transport lines that distribute the power and connect local substations with consumers [38]. Typically the process is uni-directional and focuses on providing power from the generator sites to the individual consumers. Of course, due to the nature of electricity, there is some feedback in the system but in general the communication and flow of energy or data is asymmetric. There can also be other complications, such as different electrical systems interacting with each other, for instance the frequency or other characteristics of the power can differ between geographic or legally defined areas. Even from the early days of the power grid, limitations in how electricity can be transmitted forced a configuration with many local sites that served av limited area. Because of difficulties with power transmission power often had to be generated close to where it was consumed. Taking care of all these aspects and creating national and even international power grids took a lot of planning and effort.

Technological developments like the invention and use of AC power also simplified some of the early problems related to power distribution. By standardizing the adopted technologies and configurations larger scaled systems could be created. Efficiently transferring power between different regions is needed since a localized shortage can occur or, as often is the case, the power distribution and power usage areas are far apart. Countries can also trade power with each other as any other resources are bought and sold on international markets. There are ways to share power even between countries that do not share the same power system characteristics such as first converting it to DC.

2.1 Power grid enhancements

It was also recognized early that there is a need to monitor and collect information about the state of the power grid. Readings of power information through telegraph lines started as early as the end of the 19th century [38]. In the 20th century the power lines themselves could be used to transmit data and information about the grid itself. One issue is that upgrading or changing the existing power infrastructure would result in a large costs. For instance, if a stretch of power lines should be upgraded with better communication or monitoring capabilities, this can be a very costly endeavor, especially if it has to be done for the entire power grid. Another issues is that these upgrades may have to be frequent while the desire is that the power grid, like water pipes or other fixed infrastructure, should be possible to erect and then utilize for a long period of time. A time scale that is longer than the fast pace of technological development which means retro-fitting old power lines with new systems is not always feasible or has to be done slowly due to cost. For instance power cables can be buried and adding sensors or cables for data communication in those circumstances is expensive. Because of this, techniques that utilize the current infrastructure like power-line communication are useful. Power-line communication can encode data and transmit it via the power lines, so if two sections of the grid are already connected through power lines they can also exchange data via power-line communication. In fact it can serve as a stepping stone between the old electrical grid and the modern smart grid that instead require more dedicated communication channels.

Including monitoring and control capabilities in the power grid would result in several advantages. One of these is the possibility of more easily maintaining stability in the power grid. Another benefit is detection of, and possibly automatic detection against, damage to the grid such as cable failures. Generation of power, especially from low-voltage small-scale installation such as solar panels, is also simplified as the exact input of these can be measured and utilized by the grid as needed. Detecting anomalous current flow and quickly shutting down broken or malfunctioning links can prevent damage to people or the power system itself. More advanced systems can monitor the incoming voltage to a line and compare it to the outgoing, any major differences compared to expected behaviour indicates an issue. One advantage of computerized monitoring is that the systems can be automated to repair problems on their own. In this way, the reaction time to solve issues can be considerably reduced compared to requiring human intervention every time something goes wrong. The key to implementing a system like this is to have comprehensive information on the power grid and proper communication that can relay this information and commands to a control system.

Another advantage would consist of better supervision and control of power generation. Ensuring that a generator is producing power that is in-sync, with the correct voltage and amount to the rest of the grid can also be automated. For instance the speed which the generator is spinning or how much power is fed through it can be automatically controlled. Interactions between components in the power system such as generators can cause instability and fluctuations that spread and create issues throughout the grid. Sensors can detect oscillations and anomalies in the power flow and attempts can be made to correct them by issuing control commands taking into account available sensor data accordingly. An automated system can often act quicker and with more accuracy than human operators supervising every small adjustment.

2.2 Towards smart grids

Most recently, the smart grid concept has been introduced to refer to a system where intelligent and autonomous control is implemented in individual pieces of a power grid. A brief list of common components in a smart grid are the following:

- Smart meter - Device that allows two way communication for remote management and reporting statistics.
- Data concentrator - Device in the grid that gathers and relays information from the smart meters.
- Head end system - Central system in which smart metering data relayed from the concentrators is received.
- Appliance - Device in a home that is in communication with the smart meter. For instance toaster, refrigerator, heating systems.

Figure 2.1 presents a basic high-level view of the smart grid.

Two factors are important for the functionality of the smart grid, the first one is sensing and information gathering, in other words carefully monitoring the status of the network. To be able to intelligently control the smart grid up to date information and status information on the grid is needed. For this purpose sensors and other monitoring equipment must be installed in the grid. Devices that were previously ”dumb” such as power meters must be upgraded or replaced to enable giving feedback and two-way communication. Instead of older power meters that may have to be read manually at regular intervals smart meters can instead be used that automatically report usage statistics and communicate with other components of the

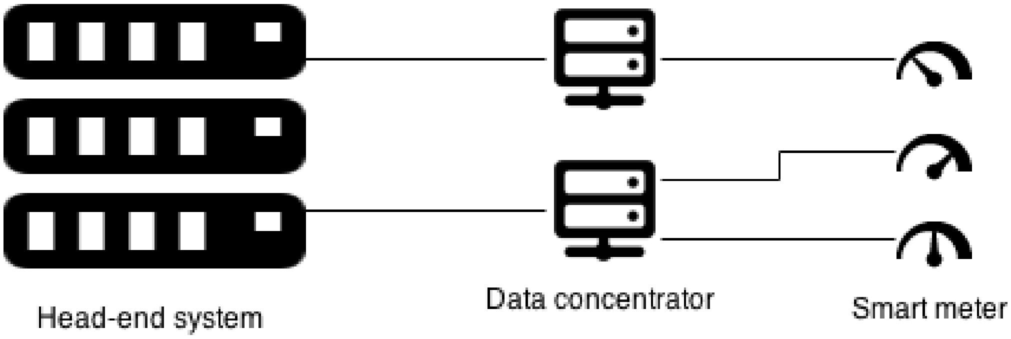

Figure 2.1: High-level view of smart grid.

power grid and home. The point of this is that all the components of the grid will be able to independently report their status to central systems. Previously there might have been a need for sending out workers to check the status of a device. If all components of the grid continuously report their status it is possible to use this information for a number of purposes such as locating faults, load balancing and in general a better overview and management of the system.

Another important functionality in the smart grid is control. To enable control there needs to be actuators and switches that can be triggered by remote commands to re-route power or change the configuration of the grid. In cases where power needs to be transmitted from one area to another or if there are power fluctuations that need to be dealt with these control systems makes that significantly easier. There also needs to be a way for smart meters to receive commands from the grid that actually affect devices in the home. Traditional meters may only transmit their metering information or even require manual readings that must be submitted by the customer. However in the smart grid meters must allow for two-way communication that allows the grid to intelligently manage not only the large components of a power system but also smaller ones down to house or even appliance levels. This can for instance allow load balancing by turning off or rescheduling certain devices from operating in a customer's home.

The benefits that the operator gains are load-balancing, locating of faults, easier billing and maintenance. Having a more complete picture of the status of the network including continuous information on the usage of individual homes and areas can simplify the provisioning of power to different areas. Getting instant updates in the case that there is a loss of power to one section of the network also helps with quickly resolving this issue. Especially identifying the location and extent of the power outage can be made easier in the smart grid because detailed information is available as to exactly which homes and devices are affected by the outage. As for maintenance identifying the exact location of the problem even down to the component that needs replacement makes it easier to send out maintenance teams to the correct location and with the right equipment. In fact sometimes it may be possible to do remote maintenance by triggering a switch or controlling the power grid with remote commands. As for load-balancing customer devices can be controlled and usage can be scheduled to be more evenly spaced thereby having more uniform power drain over the course of a day.

The smart grid gives benefits not only for the operator of the network. The customer can benefit in many ways. One way is for the power grid to inform the smart meter in a home when the price of power is low. In this way the customer can use power only when it is cheaper or at least have that information and choice available. Other benefits are that if the customer is operating a power-generating device such as small wind turbine or solar panel this energy can be easily measured and sold back to the grid or deducted from the customer's power usage. Customers can also get a nice overview of their power usage and habits to simplify reducing it. If the information captured by the smart meters is also presented in a convenient way to the customer, for instance through a web site, graphs and other statistical information can make it easier to understand what in the house and when the most power is used.

Instead of local solutions and systems that have a limited view and control a smart grid can create a comprehensive picture. The different parts of the power grid can be coordinated with each other and information about what other devices in the grid are doing is available. In this way a control system can have control and sufficient statistics to control very large grids even to a national scale. Also more advanced functionality that relies on two-way communication is possible. One example is having local devices or customers inquire and adapt their behaviour according to the current power available in the network. This can for instance be done with price incentives so that customers can schedule power consuming activities when the price of power is currently low. This can be a win-win scenario since the customers save money and the operator of the power grid has less risk of having a situation where there is a power shortage in the network or having to import expensive power from other sources to cover peak demands. Of course to what extent the provider can influence and control devices in the home of consumers is an important question with privacy implications.

Given the massive and pervasive presence of ICT security is an important factor in the smart grid. The reason for this is that now that more components include intelligent systems and microprocessors they are also susceptible to attack. Because these devices will be running software and listen for commands that they then execute the attack surface compared to traditional systems is increased. Another factor is of course that every time connection to a network is made that opens a direct communications channel into the device that can be exploited. This is especially true when any of the systems are connected to the Internet. Not only the devices but also the communication channels between them can be attacked. For instance wireless communication can be sniffed and even cables can be tapped. In this way an attacker can potentially gain access to statistical and control information on the power grid. The information found from eavesdropping can also be used to launch an attack against devices in the system.

The security aspects mentioned above mean that the smart grid as any other network connected system with devices running software and executing commands is vulnerable to attack. That fact alone means that a security solution is needed. Even more because a smart grid is a particular kind of network because it manages critical infrastructure of a country. Because of that, it is also a tempting target for attacks. By attacking the grid minor benefits such as a customer manipulation the power usage to reduce costs can be achieved. Bigger issues are attacks that try to disrupt the power grid for destructive purposes. For instance, countries can attack each other in this manner, other crimes can be simplified if the power to an area is cut, and someone may do this in order to cause the maximum amount of damage. Hence any smart grid needs a strong and comprehensive security architecture. Of course technologies used in the normal Internet can be used in addition to standard security best practices. But smart grids frequently employ custom or niche protocols that may lack built-in security solutions. There are also some special considerations specific to the smart grid like guaranteeing low latency for control channels that can have an impact on the solutions chosen.

3. Platform security for Smart Meters

Platform security relates to how security can be maintained in a specific system. Ensuring security is a complex problem and needs to be dealt not only from one point of view, but considering the whole system and even the environment in which it operates. Both the software running on the smart meter and also the hardware of the meter itself must ensure that operations are securely performed. To this end it is important to not implicitly trust any part of the system. For instance software being loaded on the meter can be compromised and the hardware of the meter tampered with. Hence it is necessary to verify and guarantee that any software that runs on the meter is properly authorized to do so. As to hardware it is necessary to ensure that the hardware provides sufficient security services and that there are checks to confirm the integrity of the hardware itself.

3.1 Software solutions

The main goal of software platform security is to make sure that the software running on a device has the permission to do so. For instance, an attacker can try to load custom software on a smart meter either by hijacking the update system or by going through an access port of the meter. Being able to run arbitrary code allows an attacker to manipulate a device and take control of it. This can include altering sensor readings, and sending fake commands to the other devices in the network or the equipment in the user's home. There are also potential attacks that exploit the compromised device as a server or a tool for attacking other systems. One common way of checking that code should be allowed to run on a device is by cryptographically signing it. Practically, the system should not trust incoming software, verifying its integrity before installation and execution, until it can verify that it is actually legitimate.

The survey paper [35] on smart meter security raises the question of who should actually own the smart meters deployed in people's homes. One issue is how to enable the smart meter to control different devices in the home. For instance, when new devices such as home appliances are released the meters may need to be updated with new software to enable control functionalities and support for them. This is also a potential security problem as a smart meter may need to implicitly trust various software from manufacturers to interact with their devices. In addition, meters from different manufacturers may be required to interact with each other.

The paper suggests to use a standardized architecture based on open source software. In particular, it refers to the OHC (Open Home Controller) model developed by the Apache foundation. The OHC works as a gateway interfacing with the devices in the home, the energy meters and the provider's devices in the energy grid. In particular the OHC should be a software package to be deployed on any class of device like a meter, gateway or even a router. The OHC would work as an open system that manufacturers can adapt or extend to contribute functionalities needed to interface different equipment with each other. The power companies and resellers can also have an open system and use the OHC as a base to implement any functionality they need. They will also have the benefit of sharing the workload for the development of this system and avoiding fragmentation. If a shared platform like the OHC is used each company is not forced to re-implement smart metering software separately. Having one standardized system like this can alleviate many of the interoperability issues, focus security research on one system instead of multiple ones and finally make it easier for manufacturers to develop drivers for smart meters.

Further techniques for ensuring integrity of a system from a software point of view are mentioned in [49]. For instance, models such as Biba & LOMAC can decide on levels of trust for different parts of a system. That is, Biba organizes software in a hierarchy ensuring that lower level processes cannot modify the data owned by higher level processes. The LOMAC model sets the integrity level of a process depending on the integrity level of the data it is interacting with. As for process integrity the paper recommends using cryptographic digest or hash functions in addition to developing the software with the latest research in safe software architecture in mind. It is also important to verify the incoming data from a communication partner as attacks and other issues can be caused by blindly trusting incoming data. Even data that appears harmless like power statistics can potentially cause issues not to mention data with actual commands to the meter.

Data integrity is also covered in [49], as to verifying collected and generated data. Collected data can be verified by means of semantic checks, through signatures or by checking whether the path the data has arrived from is secure itself. To evaluate the integrity of incoming data the source should be cryptographically verified along with the freshness of the data. Generated data is the data generated by a process, often according to previously collected data. This requires assuring that processes are also secure and non-compromised. It also depends on the integrity of the process itself as if the process is compromised the generated data will also be compromised. To this end run-time attestation and verifiable code execution can be used to protect against run-time vulnerabilities. Ensuring the integrity of a complete system is a complex task as everything from the BIOS, TPM, kernel and processor needs to be integrity checked. They all depend on each other and a flaw at any level can potentially compromise other components.

Having background processes that periodically verify the running software on a device is also beneficial [49]. This can also be coupled with hardware checks to ensure that a device running unverified code will not be able to create security associations with other parties. Furthermore, there is a relevant danger of running unsigned code such as Java, JavaScript, PDF and Flash documents in any environment that should be secure. A recent report by the security testing site AV-test shows that Adobe Reader, Flash and Java together made up 66% of vulnerabilities exploited by malware on Windows systems [21]. Many vulnerabilities are created through the use of similar third party software. For this reason, strict code signing standards should be followed to ensure that only code that has been validated can be executed. The security standards deployed should be across all levels of the network including switches, routers, field deployed units, control center equipment and servers. It is not uncommon for an attacker to target the weakest part of a system to gain a foothold from which to attempt further attacks.

With particular reference to embedded systems, two things are most important. First the manufacturer should follow standards for secure software development such as the ones recommended by CERT [43]. In addition, secure update procedures must be provided. One common way to accomplish this consists of embedding a cryptographic key in a secure storage module added during the manufacturing of the device. The hardware can be provided with the public key of a signing authority, possible under the control of the device distributor, and any download software can then be verified using this key. Approaches that check the validity of the software in such fashion, such as a kind of white-list, will make it possible to install and execute only correctly signed applications. Conversely, virus checkers trying to identify and analyze if a piece of software is malicious could potentially not be as effective.

3.2 Hardware solutions

Hardware security deals with ensuring that the hardware that a device is using is trusted. Practical solutions to achieve this rely on solutions such as cryptoprocessors and secure storage for cryptographic keys. Specifically it is crucial that, if pre-shared keys are used, an attacker cannot simply connect to the meter and retrieve the keys. Furthermore, any device attempting to interact with the smart meters has to be authorized. This is especially important if there are maintenance ports that can be used by technicians for service but potentially also by an attacker. Ensuring hardware security can be a difficult problem, but there are existing solutions to draw inspiration from, such as smart cards that can securely store keys without the possibility to extract them [SCARD]. Another method is using signatures to validate the hardware used and to periodically check its integrity.

One key feature of smart meters is the used software and hardware platforms. Usually, different companies employ different custom solutions with little reference to standards use. General purpose components such as CPUs and RAM are assembled to create essentially a computer where the smart metering software is deployed. Relying on many custom solutions can lead to security flaws because of untested components or untested combinations of components. Also, in the presence of custom hardware solutions, software may have to be custom built for the specific hardware. This which limits flexibility and the possibility for deploying the same control software on different meters. Another potential problem is that manufacturers may have to write drivers for many different variations of hardware.

That being said, a number of specific hardware requirements for smart meters have been defined [25], such as

- Support for cryptography - Enable common cryptographic operations with hardware acceleration.
- Secure key handling - Secure storeage of keys.
- Random number generators - Give random numbers to use in cryptographic operations.
- Secure clock - Correct time information.
- Trusted execution - Ensure integrity of running software.
- Tamper detection - Detect attempts to manipulate hardware or data.
- Secure debug - Provide control and only allow authorized debugging.

Hardware support for cryptography is particularly important, since cryptographic operations are usually more expensive and resource consuming when performed in software. In particular, software implementations may be too slow or expensive (in terms of energy) compared to the same operation performed via hardware. Secure key handling is another important requirement as the security of smart meters typically use cryptographic keys as a core element. Typically, a master key is used to generate other session or temporary keys for the day to day operations. This means that if the master key is compromised, the whole key material of the meter is compromised. Note that the keys must not only be protected from outside attackers but also from the final user himself, who has physical access to the meter. By reading the content of the RAM or simply files stored on the meter, keys and other important data can be retrieved. To prevent this, the CPU or other hardware components can provide special functionalities that securely store and protect keys and make them impossible to compromise. A possible solution relies on smart cards, that contain and protect the keys but allow interacting with them through a set of operations [37]. These can include public-key cryptography functionality such as authentication and signing using the keys securely stored on the card.

Furthermore many applications and communications protocols rely on random numbers or timestamps. If the clock of a smart meter is incorrectly set, operations may fail or become exposed to replay attacks. Also, some protocols require synchronization between different entities in their operation and may only accept packets within a specific time window. Hence, having a reliable and correct clock is particularly important. Random numbers are also crucial for many ciphers and security procedures. If random numbers could be predicted, freshness of procedures and information gets compromised and potential attacks can be made easier. Some attacks also try to deduce the output of random number generators by measuring time and currents in the hardware [30]. It follows that the adopted random number generator should be secure and tested to ensure random output. That is, an attacker practically perceives generated numbers as random. Secure pseudo-random number generators are implemented through ciphers.

Trusted execution is an umbrella term for a system that ensures the integrity of the software running on it from the hardware up to the software [16]. In essence, this allows the system to confirm that the operating system running on it has not been modified and is working correctly. Also any software running on the device should be signed with a correct key to ensure that it is authorized to run. This is a particularly important for smart meters, since it could be otherwise possible to load custom software, and then reporting only a subset of the occurring events, such as 9/10 of the actual power usage. Securing the hardware is also important as physical access to a device is among the most difficult aspect to protect. Since the meter is in the home, the user will have physical access and opportunity to manipulate it. By replacing or reading data from the hardware components, the the meter's operations can be compromised. Hence the meter needs to ensure that it is operating correctly without unauthorized modification. This is also related to enable secure updates of the meter, i.e. an incoming update can be signed and confirmed to be released and distributed by an authorized source. Tamper detection is also normally included in the functionality that trusted execution provides. In particular, physical anti-tampering measures such as custom screws or seals can also be employed to discourage and detect tampering attempts.

Secure debugging means controlling the rights to perform debugging of processes and only providing authorized users with this privilege. While debugging a process, its control flow and operation can be altered, because of this debugging itself can be a security risk as possible vulnerabilities in the process could be exploited or the system manipulated. The rights to debug need to be specified and the debugging entity authorized. For instance if there is a USB port for legitimate debugging or update purposes from the manufacturer/distributor of the smart meter, it needs to be sufficiently protected such that an attacker cannot connect to it and gain unauthorized access. Besides, the device connecting to the debug port needs to be authenticated [7]. This scheme can also be fine grained and allow different levels of debug access for different entities. For instance reading some statistics and usage data can be less strictly controlled compared to performing software update or maintenance.

One suggested solution consists of verifying system integrity by employing a local source like a smart card and/or a remote source like an authentication server [22]. A TPM module can also provide benefits in ensuring system integrity as it described by international standards for secure cryptography functions in processors [42]. In fact, it provides most of the functionalities mentioned in the list above, such as an RNG, key generator, hash generator and secure memory used to store encryption keys. The typical components of a TPM module are depicted in Figure 3.1. Furthermore it is also possible to rely on physical sensors to detect tampering. Finally, it is particularly difficult to detect malevolent software modifications occurring at runtime. Of course, if a remote server is used for authentication, it should be ensured that an attacker cannot impersonate this server by deploying other solutions such as communication encryption. Furthermore, in the case smart cards are used, it should be ensured that they cannot be replaced with cards containing the attacker's own keys. Attacking the key components used for security and authentication by impersonating, blocking or manipulating them can often be a powerful attack. So any source of authentication or key storage like key management servers and smart cards must be secured, authenticated and difficult to impersonate.

As suggested in [49] a secure platform such as a smart meter should verify its neighbours and communication partners by checking that they have a TPM, root of trust, secure kernel, isolated execution environment, protected storage and shielded communication channels. By checking that remote systems conform to this, a TCG (trusted computing group) can be formed where the devices have ensured the integrity of each other. Furthermore, [49] stresses that a smart grid architecture requires a comprehensive security system covering all aspects of the smart grid operation and trusted computing is only a part of this model, together with secure kernel and application layer. Two type of systems needs to be considered, embedded systems that should only run the software of the manufacturer and general purpose systems where the customer decides what to run. The former has the benefit that security and access to the device is more strictly controlled but at the same time such a solution can be less flexible when it comes to allowing extensions and adding functionalities.

Of course these functionalities can also be implemented in software. However, hardware implementa-

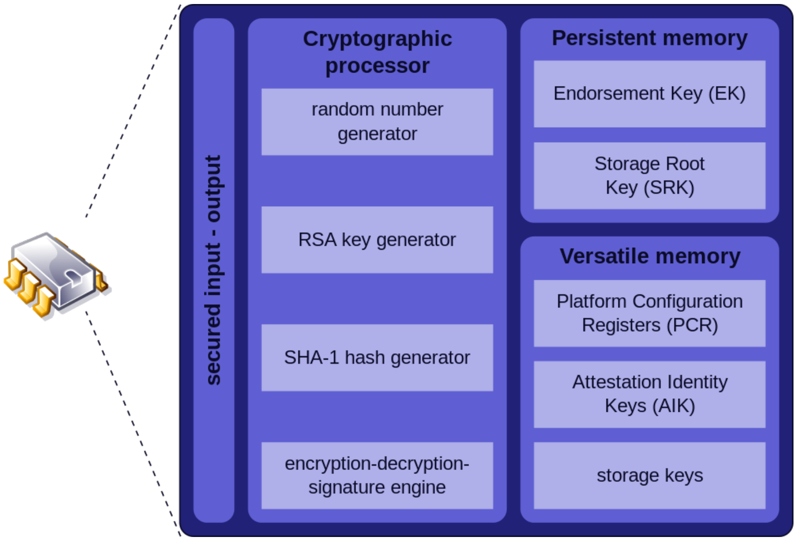

Figure 3.1: Typical components of TPM. [10]

tions are beneficial as the hardware itself can guarantee some functionality and security that software cannot always reach in terms of reliability. On the other hand hardware with specific advanced functionalities can be more expensive to acquire. Also hardware solutions are less flexible, i.e. software solutions can easily be replaced and upgraded while the hardware is less easily upgradeable. There needs to be a trade-off between price and which hardware functionality is absolutely needed. Multiple aspects like effectiveness, flexibility and price need to be considered when selecting a solution. Furthermore, some government departments set specific hardware requirements for the equipment used in smart meter, for instance the German BSI has issued a policy detailing exactly what a smart meter must provide [11]. Such requirements often stem from the fact that weak security in the smart meters and power grid of a country can be a national security risk.

3.3 Virtualization techniques

Virtualization is a technology that enables a device to be artificially split into virtual machines or be composed of virtual hardware on top of the physical hardware running the system. In this way, it is possible to logically separate processes or data in the same way as they are physically separated in hardware. A similar example is how a Ethernet switch can be separated into several by employing VLAN technology. Of course, the separation is not as strong as when implemented in hardware but if the virtualization software is correctly designed, it should prevent the same attacks and issues. So, a part of a hard drive can be designated as read-only only memory, or be set with policies that only enable processes with a specific privilege level to read from this part. Thus a part of a hard drive can be used to store sensitive data that only some processes are supposed to access. Furthermore it can be beneficial to separate the operating system and core functionality from any other process running. Then, even if a user process crashes or tries to manipulate the core system, the operating system will not be affected. This can also be combined with a technique called VMI [40] that allows for inspection of running virtual machines. VMI allows for monitoring the integrity of a virtual machine and stopping it instantly if any problems are detected.

There are certain important functionalities that it are desirable for the hardware to support, in order to create a secure environment. With new advances in virtualization and hypervisor technology it is often possible to implement this hardware-functionality in software with a similar level of security. As a consequence, special purpose-chips are no longer required and cheaper processors can be used when assembling the smart meters. Of course this means reduced cost when producing the meters, and other possible benefits like faster manufacturing and lower power consumption. There can be a demand for smart meters to support not only functionalities that come from the manufacturer but also third party tools that can even enable other functionalities. For this reason, having a system where the core functionality of the manufacturer can be protected from any other third part processes running on the devices is beneficial and often desirable. Even though virtualization is used attacks have been shown that enable an application to ”escape” from the VM and execute code on the host system [19]. In addition to that new developments in virtualization or hypervisor technology can enable implementing some of the mentioned functionality securely in software just as can be done in hardware.

4. Security Life-cycle management

One key factor in any security system is the cryptographic key material used for encryption and other services such as assuring authentication. In fact, no matter how strong any particular cipher or security scheme, in the end the security provided hinges on a correct usage and management of the key material. For instance, two devices communicating with each other can share the same key if symmetric encryption is used, or otherwise be aware of each other's public key, or at least be able to retrieve it in a secure way. No matter which solution is chosen, some initial secret information is required. In the case of symmetric encryption, this consists in pre-shared encryption keys or data to generate them. In case of public-key encryption the public keys of other devices plus possibly locations where further keys can be retrieved are necessary needed.

Another aspect is what happens and how the keys are managed after deployment of devices. It may be necessary to update keys if some changes occur in the system, for instance on a regular basis. If a key is compromised by an attacker it should not be possible to decrypt old previously captured traffic. GPG, which is a well known system for data encryption, sets an expiration data on keys it uses to limit any potential damage if the key is exposed. Keys may also have to be revoked when a device has been compromised, or suspected to be so. This can be especially difficult when considering a group of devices that share key information, such as a common group key, and sensitive data. How to securely and efficiently exclude one member of the group is an interesting problem with different proposed solutions. This chapter considers the problems of initial distribution of key material, that is imprinting, and management of key material.

4.1 Imprinting

When a new device is commissioned, it necessary that some initial data are provided. For instance, this can be a piece of information meant as a seed used to generate keys in a predictable way. Typically a given device needs something unique connected to its identity. This information can be used to identify itself and securely authenticate to other services. Of course, this makes the key material and initial provisioning of such a crucial part of the security infrastructure. If such keys are suspected to be compromised, the affected devices have to be considered untrusted and must be provided with new keys in a secure way.

Providing this initial information to a device is known as *imprinting* and can be performed by the manufacturer or independently be the operator and final owner of the device. Part of such initial information can be shared with other entities in the operator network, e.g. in order to allow secure communication. This initial information has to be accessible to the operator also. There has to be a binding between the device (such as the serial number) and the initial information assigned to a device. In this way the initial information is tied to a specific device, and its identity can be verified along with being able to use resulting key material for secure communication with this particular device. The manufacturer also has to be trusted to provide the key information placed in each device and to have strict security standards so that this information is not leaked to unauthorized entities. Thus, the manufacturing procedure has to be monitored or secured in such a way that sensitive material is encrypted or otherwise protected.

Once this initial security material has been shared, whether it is actual keys or information to generate them, it can be used to create further permanent keys or temporary session keys. When using cryptographic keys for securing communication analysis of the data exchanged or other attacks could lead to keys being exposed. Ensuring that exposed key material does not enable calculating other session keys used is important and known as forward secrecy. Also, using a key for too long makes it easier for an attacker to perform such an analysis. Therefore it is good to periodically renew keys, and use temporary session keys for specific information-exchanges. Note that specific criteria for periodical key renewal are strictly dependent of application requirements and constraints. If a key is found to be compromised it must be revoked and not possible to use in the future. Establishing group keys for communication between groups of devices is another possibility. Having an initial piece of pre-shared data enables sharing and establishing other keys or information needed for later communication in the network. The initial piece of information is needed to enable and get this process started.

As mentioned above different material can be used to generate keys. For instance this can be a serial number uniquely associated to the device. Then such initial information can be used to generate the actual key material, for instance through key-hashing functions [15]. Since the device and the key management service agree on the initial key material and security primitives, both of them can independently calculate the same keys. In this way, it could be avoided to expose the actual keys during manufacturing or at any other stage of the deployment process. It can also complicate attacks attempting to retrieve keys from devices' memory, since keys can be stored in RAM rather than in long term storage memory.

4.2 Key management and (re)distribution

Although imprinting and providing devices with initial key material is important, it is only the first step. That is most of a device's lifetime will be after manufacturing and deployment. This means that management of key material has to continue throughout the life-cycle of the device. Also, after deployment further keys may need to be generated or transmitted, the preliminary keys could be replaced or key information can be removed entirely because a device has been compromised. The idea is that compromised keys must be quickly revoked, and possibly renewed. There can also be cases when a device with valid keys is compromised and used by an attacker. In this case when a device gets compromised, and hence also the key material it contains, it is be important to quickly isolate and communicate to the other devices in the network that the specific key of the compromised device should no longer be accepted.

Of course, key management does not deal only with a particular device as to creating, removing, and updating keys. Rather, key management has to take the full network into account, so that key information is consistent and distributed correctly to all the devices. A key management system can consist of individual end-devices, key storage devices, key distribution centers and possibly certificate authorities. Typically an entity that is responsible for assigning and managing keys is present, and communicates with end-devices to refresh or revoke keys from the network. One important thing is being able to quickly revoke any possible keys when devices are compromised or suspected to be so. This is vital in order to prevent an adversary from performing a number of attacks, such as inspecting encrypted messages.

In [47], the authors consider some cyber security challenges for the smart grid including key management. They point out that a normal smart grid may have millions of credentials and mismanagement can have disastrous consequences. Furthermore they summarize important security requirements when it comes to key management, that is:

- Secure management - Managing keys in a secure fashion, correct algorithm usage, adequate key sizes and protection of crypto material.
- Scalability - The wide area systems and smart grid may have a very large number of devices which puts pressure on the system to be scalable.
- Efficiency - Computational efficiency (processing required for crypto operations), storage (disk space used for keys and RAM) and communication (overhead of crypto and metadata).

- Evolvability - Possibility for the system to be easily updated and adapted to future developments. It should be able to integrate new ciphers and protocols.

A summary of existing key management schemes is also provided, including the usage of a single shared symmetric key among all devices. If the key is exposed however the fact that it is shared among all devices means that it can lead to very severe consequences. Because of this the key should be securely stored and devices should be tamper proof to avoid the possibility for an attacker to expose the key used. Another option is *SKE* which was designed by Sandia National Laboratories for use with SCADA systems. It relies on a hybrid approach, utilizing both symmetric and public-key encryption depending on the communications scenario. One drawback of SKE is that it does not have a complete key management system nor provides good support for multicast or broadcast secure communication. *SKMA* is a system that was built to improve on SKE. A Key Distribution Center (KDC) is used for the generation and distribution of keys in the system. Using the KDC two keys are created for each device, one for node-to-node communication and one for communication with the KDC. The node-to-KDC key is installed on the node while the node-to-node key can be requested from the KDC. This protocol does not support multicast either.

ASKMA is an option for key management on SCADA systems that uses a hierarchy of keys for improved efficiency. It supports multicast communication and is efficient from a computational point of view. *ASKMA+* is a further development of ASKMA that splits keys into classes, each one of which maintains the hierarchical structure of ASKMA. Compared to ASKMA, it is more efficient in terms of storage and also better when it comes to multicast communication performance. *SMOCK* is a proposal for a lightweight key management system for wireless devices. It has very low communications overhead but is less computationally efficient and is not fully compatible with multicast communication.

An issue pointed out in [47] is that many of the key management protocols target a specific architecture such as SCADA. Certainly, the modern smart grid can include SCADA systems, but it is also a collection of various devices, often under the control of different entities. This adds additional challenges because the key management protocol has to be dynamic enough and not tied to a particular infrastructure. On the other hand, not all parts are time sensitive which means that low cost asymmetric encryption could be utilized. Scalability is also important, because of the size of the smart grid and its diversity. The various protocols used in the smart grid also come with their own challenges, i.e. some may have strong support for encryption while others can have less security functionalities built into the protocol. It is recommended that, apart from conventional PKI-schemes, alternatives like policy-based and attribute-based encryption may be interesting options to look into for the smart grid.

Support for group key management can be desirable in smart grids, since relying on broadcast/multicast communication benefits in terms of efficiency. For instance, a large number of meters can be grouped together to regularly be provided with information or updates. This means that data provisioning through multicast can be much more efficient compared to unicast communication. A smart grid is also usually hierarchical where devices are organized in levels and the devices at the top need to send information to the other ones at the bottom. So having a single or a few sources originating data that is to be sent to the smart meter at the bottom of the hierarchy is a common occurrence. Because of this, multicast support from key management protocols is an important and desirable feature.

In addition to the periodical key renewal discussed above, in the case of group communication it is important to renew a given group key upon the occurrence of the two following events. *1)* In case a new device joins the group, so that it is not able to access any group key used before its joining. This prevents the device to access old communication within the group, so assuring the backward security requirement. *2)* In case one or more devices leave the group, i.e. they ask to leave or have to be evicted because are compromised or suspected to be so. In particular, the group key must be revoked, and a new one must be distributed to the remaining group members. This prevents the leaving devices from taking part in future communication within the group, so assuring the forward security requirement. It is vital to assure that the leaving devices are not able to participate to the key re-distribution process, and thus cannot get the new group key. This can be particularly difficult in case multiple, possibly colluding, group members have to be evicted at the same time. Finally, a group key management scheme must be highly efficient and scalable with the group size, in order to limit the impact on system performance, and allow the network to be fully operative again as soon as possible. The reader can refer to [3][5][12][13][31] for some relevant examples of available group key management approaches.

4.3 Open problems

One factor mentioned in [47] is that key management support for systems using symmetric keys is lacking. Many of the key management systems listed in the preceding section use asymmetric or hybrid approaches. For symmetric keys that can have a benefit in terms of calculating power required there is a need for more key management solutions. Symmetric keys have to be changed periodically and this means that a key management system has to provide new keys to the devices in the network. This can also open additional security vulnerabilities as the keys can be exposed in transit. There also has to be a trust system in place that can authenticate the device to the provider of new symmetric keys and vice versa. Limiting the data protected by a symmetric key could be one way to alleviate some of the drawbacks of symmetric key use and reduce the frequency of which it has to be renewed.

Another issue mentioned in the same paper is how to create a key management system that is highly scalable. Smart grids frequently have a very high number of devices in the network which means that any key management system has to be able to deal with the possibility of having to store a large amount of keys and handle a lot of key management traffic. Smart grids can also be quite diverse so the key management system must be able to handle a wide variety of devices and technologies used. For instance a lot of the key management protocols mentioned in the previous section are focused on SCADA but a key management system for the smart grid must be broader than that. Using public key cryptography as SMOCK does to improve scalability may not be the best option for the smart grid as it introduces asymmetric encryption that can be too computationally expensive for low capacity smart meters.

5. Communication Protocols

A smart metering system is composed of several interacting parts. Together with smart meter devices, many other components are present and interacting with each other. This allows enriching the whole power infrastructure's capabilities, e.g. to perform advanced remote control and data collection. This chapter covers some elements of smart metering systems, focusing on how its different components communicate with each other. Figure 5.1 shows some of the elements of a smart grid.

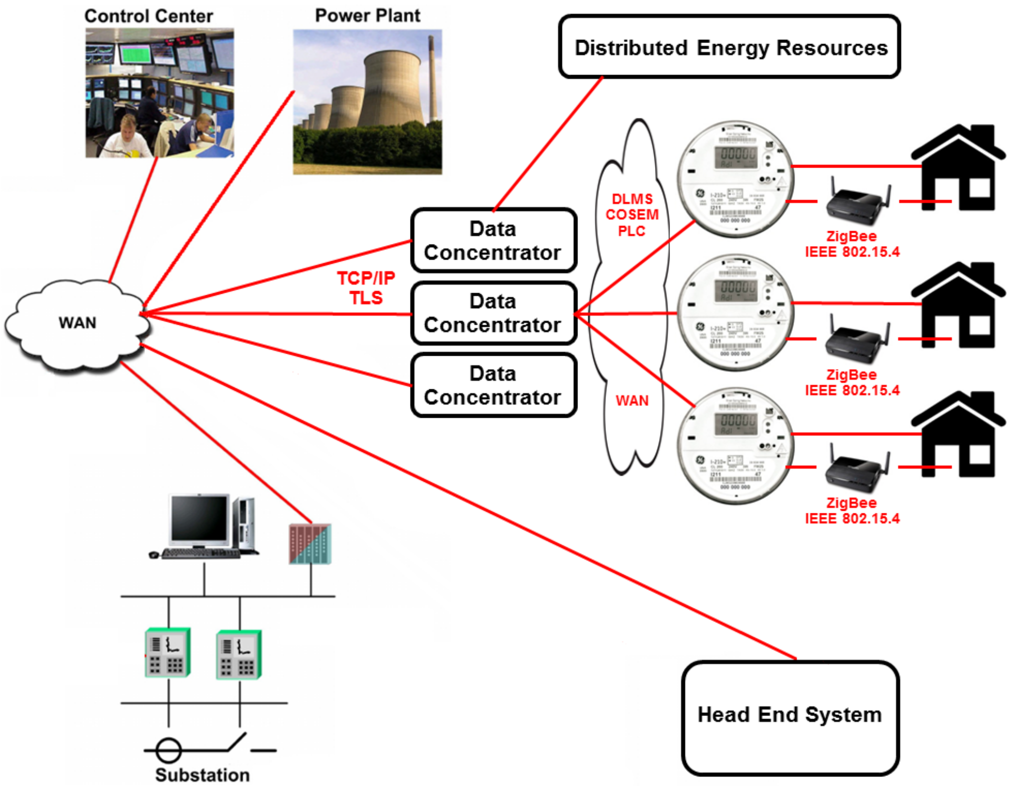

Figure 5.1: Overview of smart grid configuration.

Typical elements in a smart metering system are:

- Home appliances - They are the devices that the a customer uses in his own private home and that can interact with the smart meter. For instance, they can include lighting systems, household appliances, heating systems, and automated blinds. They can communicate and cooperate with each other, and provide statistic information. Also, they can be remotely controlled by the smart meter. In the end, these devices can react to instructions from the smart meter such as information on when power costs are low or allow the user to remotely control these devices in the home. For example, they can be selectively switched off, or set to a convenient consumption schedule.

- Smart meter - These devices are distributed to the end users, and allow for the smart power grid to gather data and perform management and control operations remotely. In essence, they work as home gateways to the smart grid. That is on one hand it is connected to private home appliances, which it can interact for monitoring and other purposes. On the other hand it is connected to the main power grid, and can in turn receive monitoring requests and other commands. There are various configurations where a smart meter can be a standalone device with a dedicated metering function. As an alternative, the smart meter can integrate network functionalities and additionally act as a ”gateway”. In such a configuration no extra separate gateway device is needed for providing network connectivity.

- Utility meter - The actual meter that measures the consumption of electricity, gas, water etc. can be a standalone device or be implemented as several devices that in turn communicates with the smart meter. These devices may need to be installed in specific areas, and are often provided by the specific utility company. Hence, they require a communication interface to to transmit their information to the main smart meter.

- Gateway - It is an optional device that acts as communication gateway with the rest of the smart grid interfacing with the smart meter in the house. Having tit as a standalone devices can simplify the configuration in some scenarios and could allow the use of common hardware such as routers to fill this role. As mentioned the gateway can be integrated with the meter but currently it is common to deploy it as a separate device.

- Data concentrator - It is located between smart meters and the central infrastructure of the energy provider. Its main purpose is to collect and aggregate data from the smart meters, and act as a relay between the central control systems and the individual meters. It is beneficial to have such an intermediate component in order to separate the network into sections. For instance, one data concentrator can control all smart meters in a specific geographic or administrative area. Data concentrators then connect to the central systems, lessening the load on them. This is a better option than having every individual smart meter being connected to the central systems.

- Head-end system - These make up the central control systems for the smart grid. It is connected to individual data concentrators through which it can collect statistic reports and perform remote operations. One key functionality is of course gathering statistic information coming from smart meters, which allows the energy providers to correctly charge the end customers. Remote control of smart meters and power switching in the power grid are additional functionalities. A central system can be under the control of one company, that then provides access to market providers. Remote updates or maintenance commands can be dispatched from central systems to the smart meters. Alternatively, data concentrators can directly update smart meters.

The following section provides an overview of the communication between the discussed components. The rest of the chapter presents the most commonly referred communications protocols.

- Communication between smart meters and home appliances - This is required to allow remote control of home appliances and collect data from them. Also, this allows to lessen the load on the power systems in case of low power situations, or home appliances to make intelligent decisions on when to switch on, depending on the current status of the power grid and the current power cost.

- Communication between smart meters and data concentrators - In essence commands and metering information are conveyed between individual smart meters and data concentrators. This can alleviate some of the burden on the centrals systems and also allow for collecting statistics and performing maintenance operations.

- Communication between data concentrators and central head end systems - For this case data concentrators relay information to or from the smart meter with the central infrastructure of the energy provider. The data concentrators are connected to individual smart meters, and the data concentrators themselves then connect to the central head end part of the network. In this way the devices are structured in a hierarchical system.

- Other potential communications channels - They include administrative access to smart meters for technicians, direct communication between smart meters and central head end systems, communication between smart meters and external gateways or utility meters.

5.1 Smart meters and smart home appliances

Communication between a smart meter and the associated home appliances differ in many ways between communication from the meter to the outside world. This is due to the fact that the bandwidth required for sending simple commands to devices in the home is generally low and that mobility of appliances is an important factor to consider. Thus, the protocols used for smart meter to appliance communication rely on wireless techniques and can be short range protocols that only operate within a certain physical range. It is preferable that communication protocols are energy efficient, especially in the presence of battery-powered appliances. Having battery constrained appliances need not be a problem as the bandwidth needed can be quite low and using short range communication can often save battery power in devices. As some appliances can be power constrained these can prove to be advantageous. There is a wide range of protocols used for in house communication. Some are explicitly intended for low power networks, while others are more common technologies such as IEEE 802.11 (WiFi). Also some of these protocols have wider usage or were originally made for different purposes while some have been specifically designed with smart grids in mind.

In the following section, an overview of this class of communication protocols is provided.

DPWS (Devices Profile for Web Services)
DPWS is a set of standards including WSDL, SOAP and XML [27] and it is an OASIS standards since 2009. Its purpose is to provide web services in a secure way, with focus on constrained devices. The four main goals stated in the specification for DPWs are; sending secure messages to and from a service, being able to dynamically discover a web service, creating a description of a web service, and finally subscribing to events from a service. DPWS defines a minimum set of requirements to achieve these functionalities. It uses SOAP over UDP to perform message delivery and relies on a protocol called WS discovery that enables discovering existing web services on a network [28]. WS discovery can use multicast to listen for available services on a network. Whenever a device running a service joins the network, it will announce its presence to a specific multicast group.

6LoWPAN
This is a protocol which focuses on providing networking functionality in sensor networks. As ZigBee, it also operates on top of 802.15.4. Benefits of 6LoWPAN are a reduced memory overhead and the IPv6 header compression to reduce the communication overhead. In general 6LoWPAN is particularly useful in networks of resource constrained devices. Also, the support for IPv6 allows devices to be accessible from anywhere on the Internet through its own IP-address. This in turn allows devices to be independent and not have to rely on a gateway or communications proxy. For instance, ZigBee nodes require an intermediate gateway device and cannot be directly reached from outside the local network through their personal addresses.

KNX
KNX was created by a consortia of three companies working in the area of home control, namely Batibus, EIB and EHS. KNX is also defined as an ISO standard in ISO/IEC 14543-3-x [48]. It is intended mainly for communication within intelligent buildings, and it relies on another standard for managing electrical device, European Installation Bus (EIB). Also, it supports a wide array of communication media such as copper cable, radio and infrared communication [18]. KNX can support both multicast and unicast configuration, making possible group communication and control. The KNX specification is not freely available, but has to be purchased through the KNX association. KNX is frequently deployed together with sensors to create

a control system that can monitor a building for alerts from fire, burglary or other malfunctions. There are several examples of deployments with management interfaces in Sweden utilizing KNX [17].

ZigBee/IEEE 802.15.4

ZigBee operates wirelessly on top of the IEEE 802.15.4 standard [6]. In turn IEEE 802.15.4 specifies rules and the physical layer for personal area networks, considering communication ranges of approximately 10 meters. Communication is in the unlicensed 2.4 GhZ spectrum and thus does not conflict with any regulation issues. The ZigBee SMart Energy Profile defines specific functionalities and messages as a protocol for monitoring energy and water systems. ZigBee Smart Energy V2.0 adds support for electric vehicles and such upgrades that further integration with smart homes [50]. ZigBee is a quite lightweight and cheap system and can be cheaper to deploy compared to WiFi and Bluetooth. Although the one-hop physical transmission range is limited, longer distance transmissions can be accomplished by means of multi-hop and mesh network topologies.

IEEE 802.11/WiFi

One option is to simply use the common IEEE 802.11 protocol commonly referred to as WiFi. It is a well consolidated technology with wide hardware and software support. Employing WiFi means that individual appliances require a WiFi card and connect to a home wireless network. Devices like smart phones, pads, TVs, and even some household appliances like refrigerators already come with WiFi. In this way less intermediate technologies are needed between the devices and the existing home network or even the Internet itself. Every device can have a public IPv6 address where it is accessible, this is in contrast to ZigBee for example which uses its own addressing and needs translation to reach IP-devices on the Internet. A drawback is that relying on WiFi can be costly from a manufacturing standpoint and energy requirement point-of-view. If all devices down to the level of light bulbs must implement a WiFi-circuit it raises the cost of manufacturing. Interference may also be an issue if a large number of wireless nodes are considered. Since the transmission range of WiFi is wider compared to Bluetooth or ZigBee, interference with other neighboring users may also be a problem. From a security perspective WPA2 provides strong security in terms of encryption and integrity protection. Of course, this results in additional communication overhead and energy consumption.

BACnet

BACnet is another protocol to enable devices in a building to communicate with each other. It defines objects and services that can be utilized for this purpose. For instance, there are discovery services that enables finding other BACnet devices, and a large number of objects that can be used to retrieve information from a device. If these standardized objects are implemented other entities can use these objects to read information from a device. In this regard, BACnet is similar to SNMP [24] where there is an attempt to standardize what information a device should provide and how. For lower layers, BACnet supports a number of technologies such as Ethernet, LonTalk and point-to-point links [26]. An open source implementation of BACnet is available for download [39] and BACnet is an ISO standard. BACnet also includes optional network security that can provide encryption and authenticity of traffic by means of symmetric cryptographic keys. Keys are always distributed as pairs, i.e. one encryption and one signing key. In total, there are 6 kinds of these pairs used for different purposes. Messages can be signed with an HMAC based on MD5 or SHA256, while optional encryption is performed with AES.

LonTalk

LonTalk is a protocol developed by Echelon and is available as a standard under ISO/IEC 14908. It is part of a more comprehensive system named LonWorks, that is a software/hardware platform to develop control systems. It can be used for building automation with regards to energy, heating and air conditioning. Methods exist to make LonWorks-based systems interoperable with BACnet, Modbus and KNX [36]. They also provide support for integrating LonWorks-based networks with conventional IP-networks. LonWorks is quite diverse and used in a wide variety of applications. For instance the some subways systems use LonWorks for brake controls [41]. Echelon has their own microprocessor that implements the LonTalk protocol.

Bluetooth

Bluetooth is a short range communications standard for Personal Area Networks (PAN) [1]. It uses the same frequency bands as WiFi but with lower transmission power and shorter communication range. While WiFi considers a centralized Access Point (AP) that provides access to the network. Bluetooth relies on a distributed approach where devices connect directly to each other. Bluetooth is designed to reduce configuration efforts and to be fast to set up and operate. From a security point of view historically Bluetooth has had a number of vulnerabilities [20]. However later updates to the protocol such as Bluetooth v2.1 provides improvements when it comes to security such as requiring encryption for communication between devices. For security services it uses the SAFER+ cipher which was one of the candidates submitted for becoming AES.

5.2 Smart meters and data concentrators

Some protocols rely on dedicated channels only for transmission of control data. However others reuse the existing electrical system allowing communications data to be sent over the power lines. This can have the advantage of reusing existing infrastructure, but displays a limited bandwidth for communication. Of course robustness is also lessened, since if power lines have any issue, the control traffic will also be affected. On the other hand an existing Internet connection is very frequently available so making it possible to rely on other more efficient communication protocols. In such a case, there is also less need for intermediate devices that translate between different protocols. The rest of this chapter overviews some common protocols for communication between data concentrators and smart meters.

DLMS/COSEM

DLMS (Device Language Message Specification) is a general application layer protocol for defining resources and access methods [8]. COSEM (Companion Specification for Energy Metering) is the energy meter specific addition that specifies common objects related to smart meters. COSEM attributes describe objects and can be manipulated with specific interfaces. DLMS/COSEM is attempting to be a general standard not only for electricity metering but also for heat, gas and water management. The protocol is based on a client/server architecture where the collection systems pull information from the smart meters. Also, it supports different underlying communication methods through ”profiles”. Profiles enable DLMS/COSEM communication as an added layer and is used with different options depending on the underlying technology [9].

SML

RWE, EON and EnBW have jointly developed the SML protocol as a part of the SYM^2 project [46]. SML was designed by German companies is currently mostly used in Germany. It can be used on top of TCP/UDP and its application layer defines a structure for sharing data between the measurement point and collection center. The structure defined in the protocol is usable both with packet-oriented networks and communication over GSM [23].

IEC 61334-5 PLC

This protocol relies on existing power lines for communication [29]. While they are conveying AC current they can at the same time carry a limited amount of information. In principle, they add a signal to the carrier that has been modulated [4]. This carrier signal is then used to encode the data to be transmitted. This protocol is a part of the IEC 61334 standard for power line communication. The actual throughput of this protocols is relatively limited due to the few bits of information sent in each power line cycle. The length of a cycle depends on the utility frequency which is 50 Hz in Europe giving a cycle length of 1/50 seconds. In general upper level protocols such as DLSM/COSEM can be deployed on top of IEC 61334-5 PLC. Also, using OFDM (Orthogonal Frequency-Division Multiplexing) techniques can boost the amount of throughput it provides, potentially giving near broadband level performance [4].

SITRED
The SITRED protocol is also based on PLC, and was first developed in Italy in the 90s [2]. It works in a similar manner to IEC 61334-5 PLC and supports both the SITRED and the LonTalk protocols. This enables some interoperability between LonTalk and SITRED systems. The data rate is quite limited, i.e. 14.4 kbit/s. In 2009 SITRED was released as open source software by its creator Enel to encourage its adoption [33].

PRIME (Powerline Related Intelligent Metering Evolution) PLC
This protocol also relies on power lines. It provides a maximum data rate of 130 kpbs, and there are compatibility layers that provide functionality for both IPv4 and IPv6 [32]. Thus, TPC/IP traffic can be sent on top of PRIME PLC. However, PRIME cannot coexist well with IEC 61334-5 PLC in the same network. Currently, the PRIME alliance states that over 5 million meters using this protocol have been deployed. PRIME PLC version 1.4 was released as late as October of 2014, there is a quite active development process ongoing. PRIME is an open standard.

5.3 Data concentrators and central head-end systems

Data concentrators are responsible for aggregating and relaying data collected from the smart meters. This aggregated data and statistics are then transmitted to the head-end system for further processing. Furthermore data concentrators can relay commands from the head-end systems to the smart meters. For instance, the head-end systems can send a command to a number of concentrators, which in turn forwards the command to the meters they are connected to. So doing the load can be lessened on the head-end systems, avoiding continuous end-to-end communication with the smart meters in the system. Concentrators can also be used to provide large amounts of data such as software updates to the meters. Since data concentrators are supposed to be provided with adequate communication and energy resources, they can rely on traditional Internet connections or mobile links over GSM/GPRS to interact with the head-end-system. The data amounts being transmitted here are larger compared to the ones between the meter and concentrator because the concentrator has to report data from a large number of meters. This also sets a requirement on the type of connection provided to assure sufficient bandwidth.

Internet
One way to connect the data concentrators to the head-end systems is directly through the Internet. In many cases an Internet connection available in the areas and neighborhoods where data concentrators are located. Compared to PLC solutions, this allows achieving higher data rates and to be independent from the power lines. Another benefit is that security protocols such as TLS, IPSec can be utilized to secure communication. These standards are well consolidated widely adopted and utilizing them can be better than any custom less adopted solution. However, there can be a potential risk of eavesdropping if the traffic is routed through systems that the operator does not have control over. Smart grids and their components can be an attractive target for attackers, and components directly connected to the Internet are also exposed to automated scans for vulnerabilities, worms, and DoS attacks.

GSM/GPRS
If an Internet connection is not available, the cellular network can be used for communication. This can be useful in case of more remote areas where Internet connectivity is not available. The cell phone network typically extends to areas that are remote and only lightly populated, or not even populated at all. GPRS can reach data rates of around 150 kbit/s [14] which is lower than broadband Internet connections but faster than other solutions such as PLC. It may also be possible to improve performance by considering 3G or 4G mobile communications.

DLMS/COSEM
DLMS/COSEM can also be used for interfacing the data concentrator and head-end system.

6. Secure Communication

As any network connected device, smart meters are vulnerable to a number of attacks. Any time a device interacts with others, and especially when it receives commands and instructions from other devices, security risks arise. Thus, it is crucial for smart meters to verify any incoming commands. In addition, there is also the risk that the attacker and end user coincide which makes securing the system even more complicated. The devices in the network should not generally assume that each other are trusted. In particular, smart meters should verify that incoming messages are sent by an authorized entity in the network. Similarly other devices in the energy provider's network should verify the identity of smart meters to ensure that no impersonation attack or transmission of fake data occurs.

6.1 Threats

Smart meters are in essence vulnerable to a number of attacks against general purpose devices. A smart meter is a computing device which can use the same communication protocols as many other devices for communication. In such cases the overlap between attacks against a general Internet-connected device and a smart meter is quite large. According to [22], some common attacks against smart metering are:

- Message eavesdropping - Monitoring traffic and exchanged messages.
- Denial of Service (DoS) - Flooding device with messages.
- Metering report forgery - Creating false metering data.
- Injection of fake messages - Creating false command data.
- Compromising meter integrity - Attacks against the meter itself.

Some attacks have purely destructive purposes, some can be performed for the financial benefit of the end user and others aimed at and penetrating deeper into the infrastructure of the smart grid. Message eavesdropping consists in listening to the traffic sent to and from smart meters. In cases when wireless communication is used, this is particularly easy as communication can be intercepted by anyone in transmission range. Even when wired systems are used, it is possible to connect into the cable and monitor traffic. Figure 6.1 shows a fiber optic tap that can be used to eavesdrop an active link. This kind of attack can be simply performed by curious neighbours or possible thieves interested to know the owner is home and what devices he owns.

Denial of service is another common attack. A denial of service attack consists of overloading a receiver with messages that it cannot parse fast enough, thereby flooding it with data. This attack can be targeted at individual smart meters, or more likely, the energy providers' infrastructure. SYN flooding and SSL/TLS-handshake attacks are two examples of denial of service attacks. Furthermore, a number of jamming attacks can be performed, by interfering at the physical layer in the presence of wireless communication. A denial of service attack can result in seriously disrupting the energy provider infrastructure, which can be prevented from gathering monitoring information or executing control operations. In such a case, the entire smart grid can be affected. Also, smart meters can be vulnerable to DoS attacks and may have difficulty withstanding message flooding from a sufficiently powerful attacker.

Forgery of smart metering reports can consist of manipulating measurements sent by smart meters or even generating counterfeit messages. Possible motivations include reducing the electricity bill of a

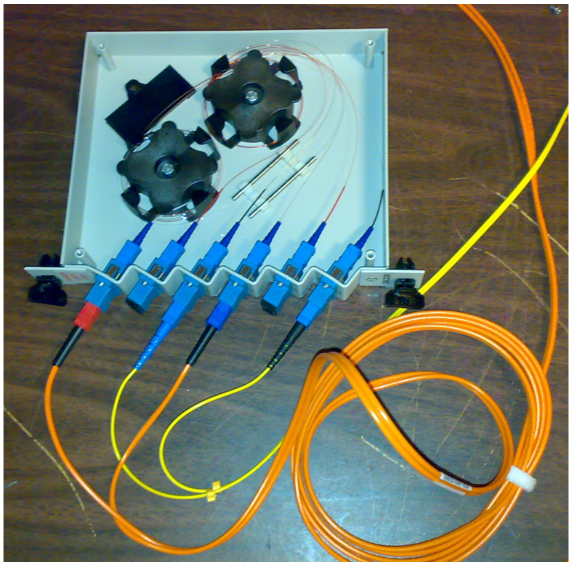

Figure 6.1: Fiber optic tap. [34]

customer or increase the electricity bill of a specific victim. Practically this can be achieved by intercepting report messages and then either changing their content or discarding them. The attacker can also be the customer which means direct access to the smart meter and cabling is available.

Injection of false commands is a an attack where collected messages, containing commands to a smart meter, can be altered, and new ones can be injected. The impact of this is that an attacker can execute operations and otherwise influence the smart meters. Smart meters provide a range of commands to perform operations such as controlling home appliances. As a particular case, an adversary can replay old collected messages and induce smart meters to repeatedly perform specific actions. If an attacker for instance captures a command that tells the meter to shut down certain devices the attacker can replay these.

Note that message forgery and injection becomes even more effective in case an adversary manages to compromise and take control of a network device. In such a case, as long as they are not detected, compromised devices can considerably simplify the attacks execution and increase the effect and impact. The attacker can also send commands from the smart meter to appliances or use the meter as a starting points for attacks deeper into the building network. A homogeneous network can also make it easier for an attacker to employ automated scanning tools and reuse attacks methods against many targets.

6.2 Solutions

Several techniques for establishing communication can be adapted or deployed in smart grids. One of the main solutions recommended in [22] is using encryption for communication between entities in the network. This would practically solve many of the problems listed in the section on threats. If network traffic is encrypted, eavesdropping becomes significantly harder. Of course an attacker can still capture the data being sent but since it is encrypted it will have limited use. There are many current systems available to implement encryption from TLS to IPsec that could be deployed in smart grid networks. Of course different devices have different requirements and the encryption used should be adapted to the capabilities of the device, type of communication (wireless/wired) and layer at security is required. There are systems that ensure link-layer security between the hops in the network and others that provide end-to-end security services. Of course it is also possible to deploy a combination of these to have security at multiple layers of the communication.

Similarly spoofing attacks and injecting false data in to the system is more difficult since receiver would require the data to be encrypted with a specific key for it to be accepted. Replay attacks could still be possible where an encrypted command is captured and retransmitted later to influence the systems. Because of this encryption should be coupled with authentication and integrity to ensure that the sender is authorized to execute commands and that the contents of the message has not been manipulated. Systems such as IPsec and TLS provide this service too however one issue is key distribution and if a central authority should be used for signing keys as is done with TLS.

Denial of service attacks is a difficult problem since when if traffic is blocked at the receiver resources will be expended and upstream systems can be overloaded so legitimate traffic is not let through. Because of this dealing with denial of service attacks is often best done if the traffic can be blocked as close to the sender as possible. This means involving other systems than the one under attack to cooperate in blocking the attackers traffic. There are also methods where the receiver can attempt to filter messages or even stop receiving traffic in cases of attack. However finding an effective counter measures for theses kinds of attacks remains difficult.

Sandboxing is a potential solution for attacks against smart meter integrity. In essence sandboxing consists of isolating processes running in the meter from each other. This means that a security issue in one part of the software on the meter or attacks performed via hardware can be limited. It is especially important to keep the operating system and core functionality separated from less privileged processes. This can also help in cases where third party developers need software to run in the smart meters, for instance to interact with their home appliances. Hardware solutions like TPM and smart cards can also be utilized to ensure system integrity and verify running code. Intrusion detection systems are really important in case smart grid devices become physically or logically compromised. They can monitor the system and try to detect signs of attacks or anomalous behavior. If such behavior is detected automatic actions can be performed to isolate or repair the affected devices.

6. Bibliography

[1] Bluetooth Special Interest Group. Specification of the Bluetooth system. https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439.

[2] Brunello Botte, Vincenzo Cannatelli and Sergio Rogai. The Telgestore Projet in ENEL's Metering System. June 2005. http://www.cired.net/publications/cired2005/papers/cired2005_0406.pdf.

[3] Chung Kei Wong, Mohamed Gouda and Simon S. Lam. Secure Group Communications Using Key Graphs. *IEEE/ACM Transactions on Networking*, 8(1):16–30, February 2000.

[4] Cypress Semiconductor. What is Power Line Communication?, August 2008. http://www.eetimes.com/document.asp?doc_id=1279014.

[5] Debby M. Wallner, Eric J. Harder and Ryan C. Agee. *RFC 2627, Key Management for Multicast: Issues and Architectures*. Internet Engineering Task Force, June 1999.

[6] Digi International. *Demystifying 802.15.4 and ZigBee*, 2009. http://www.digi.com/pdf/wp_zigbee.pdf.

[7] Discretix. Secure Debug, 2013. http://www.discretix.com/secure-debug/.

[8] DLMS User Association. COSEM interface classes and OBIS identification system.

[9] DLMS User Association. *DLMS/COSEM Architecture and Protocols*, July 2014. http://dlms.com/documents/Excerpt%5FGB8.pdf.

[10] Everaldo Coelho and YellowIcon. File:TPM.svg, September 2008. http://commons.wikimedia.org/wiki/File:TPM.svg (Released by Everaldo Coelho and YellowIcon under the LGPL license).

[11] Federal Office for Information Security. *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*, March 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0073b_pdf.pdf.

[12] Gianluca Dini and Ida M. Savino. LARK: A Lightweight Authenticated ReKeying Scheme for Clustered Wireless Sensor Networks. *ACM Transactions on Embedded Computing Systems*, 10(4):41:1–41:35, November 2011.

[13] Gianluca Dini and Marco Tiloca. HISS: A HIghly Scalable Scheme for Group Rekeying. *The Computer Journal*, 56(4):508–525, April 2013.

[14] GSMArena. GPRS - Mobile terms glossary - GSMArena.com, 2015. http://www.gsmarena.com/glossary.php3?term=gprs.

[15] Hasen Nicanfar, Paria Jokar and Victor C.M. Leung. Smart Grid Authentication and Key Management for Unicast and Multicast Communications. In *IEEE PES ISGT ASIA 2011 Conference*, November 2011. https://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/13.pdf.

[16] James Greene. *Intel Trusted Execution Technology*. Intel Corporation, 2012. http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf.

[17] KNX. KNX Association ::[SE-Official website] KNX Sweden Referencesobjekt, January 2009. http://www.knx.org/se/knx-sweden/referencesobjekt/.

[18] KNX Association. What is KNX?, 2014. http://www.knx.org/knx-en/knx/association/what-is-knx/.

[19] Kostya Kortchinsky. Cloudburst: Hacking 3D (and Breaking Out of VMware). In *Black Hat USA 2009*, July 2009.

[20] Marek Bialoglowy. Bluetooth Security Review, Part 1, November 2010. http://www.symantec.com/connect/articles/bluetooth-security-review-part-1.

[21] Markus Selinger. *Adobe & Java Make Windows Insecure*. AV-TEST GmbH, December 2013. http://www.av-test.org/en/pdfnews/7.

[22] Martin Erich Jobst. Security and Privacy in the Smart Energy Grid. In *Proceedings of the Seminars Future Internet (FI), Innovative Internet Technologies and Mobile Communications (IITM), and Autonomous Communication Networks (ACN)*, pages 159–164, Munich, Germany, July 2013. Technische Universitt Mnchen. http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2013-08-1.pdf.

[23] Martin Wisy. *SML, Smart Message Language Version 1.02*, January 2008. http://www.vde.com/en/fnn/extras/sym2/Infomaterial/documents/sml_080711_102_eng.pdf.

[24] McCloghrie, Case, Rose and Waldbusser. *RFC 1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*. Internet Engineering Task Force, January 1996.

[25] Meera Balakrishnan. *Providing Security for Smart Energy Systems: An Industrial White Paper*. Freescale Semiconductor. http://cache.freescale.com/files/industrial/doc/white%5Fpaper/SESECURITYSEWP.pdf.

[26] Michael Newman. BACnet: Answers to Frequently Asked Questions, October 1998. http://www.bacnet.org/FAQ/HPAC-3-97.html.

[27] OASIS Web Services Discovery and Web Services Devices Profile (WS-DD) TC. *Devices Profile for Web Services*. OASIS, July 2009. http://docs.oasis-open.org/ws-dd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.pdf.

[28] OASIS Web Services Discovery and Web Services Devices Profile (WS-DD) TC. *Web Services Dynamic Discovery (WS-Discovery)*. OASIS, July 2009. http://docs.oasis-open.org/ws-dd/discovery/1.1/os/wsdd-discovery-1.1-spec-os.pdf.

[29] OPEN meter Open Public Extended Network metering. Description of State-of-the-art PLC-based Access Technology. May 2009. http://www.openmeter.com/files/deliverables/OPEN-Meter WP2 D2.1 part2 v2.3.pdf.

[30] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. http://www.cryptography.com/public/pdf/TimingAttacks.pdf.

[31] Peng Liu, Wang-Chien Lee, Qijun Gu and Chao-Hsien Chu. KTR: An Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services. *IEEE Transactions on Dependable and Secure Computing*, 6(3):188–201, 2009.

[32] PRIME Alliance Technical Working Group. *Specification for PoweRline Intelligent Metering Evolution*. PRIME Alliance, October 2014. http://www.prime-alliance.org/wp-content/uploads/2014/10/PRIME-Spec_v1.4-20141031.pdf.

[33] Roberta Bigliani. Enel Makes its Smart Meters ”Open Source”, October 2009. https://idc-community.com/energy/smart-grid/enel-makes-its-smart-meters-open-source.

[34] Roens. File:Fiber optic tap.png (http://creativecommons.org/licenses/by-sa/2.0/deed.en), November 2007. http://commons.wikimedia.org/wiki/File:Fiber_optic_tap.png.

[35] Ross Anderson and Shailendra Fuloria. Smart meter security: a survey. http://www.cl.cam.ac.uk/ rja14/Papers/JSAC-draft.pdf.

[36] Sierra Monitor Corporation. Introduction to LonWorks Control Network Protocol, October 2015. http://www.sierramonitor.com/connect/protocol-gateway-integrators/lonworks.

[37] Smart Card Alliance. Smart Card FAQ. http://www.smartcardalliance.org/smart-cards-faq/.

[38] Stephen F. Bush. *Smart Grid - Communication-enabled Intelligence for the Electric Power Grid*. John Wiley & Sons, Ltd (IEEE Press), 2014.

[39] Steve Karg. BACnet Stack - An open source BACnet protocol stack for embedded systems, October 2013. http://bacnet.sourceforge.net/.

[40] Tal Garfinkel and Mendel Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In *The 10th Annual Network and Distributed System Security Symposium*, February 2003. https://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/13.pdf.

[41] Transportation Systems Design, Inc. IEEE-1473-L & Safety Critical Applications. http://www.tsd.org/ieee1473/safety/index.htm.

[42] Trusted Computing Group. Trusted Platform Module (TPM) Summary. http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary.

[43] United States Computer Emergency Readiness Team. CERT Coding Standards, March 2015. https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards.

[44] U.S.-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. April 2004. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[45] U.S. Department of Energy. Smart Grid — Department of Energy. http://energy.gov/oe/services/technology-development/smart-grid.

[46] VDE Association for Electrical, Electronic & Information Technologies. A joint initiative for technological innovation. http://www.vde.com/EN/FNN/EXTRAS/SYM2/Pages/default.aspx.

[47] Wenye Wang and Zhuo Lu. Cyber security in the Smart Grid: Survey and challenges. *The International Journal of Computer and Telecommunications Networking*, 57:1344–1371, April 2012. http://www.ece.ncsu.edu/netwis/papers/13wl-comnet.pdf.

[48] www.konnex.org. KNX has become an International Standard: ISO/IEC 14543-3. http://www.knx.org/fileadmin/downloads/07 - News & Press/03 - Press Releases/01 - English/KNX is International Standard.pdf.

[49] Ye Yan, Yi Qian, Hamid Sharif and David Tipper. A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials*, 14(4):998–1010, 2012.

[50] ZigBee Alliance, Inc. *Smart Energy Profile 2 Application Protocol Standard*, April 2013. http://www.zigbee.org/?wpdmdl=2127.