CYBER PHYSICAL SYSTEMS SECURITY IN SMART POWER GRIDS

PROJECT THESIS

Submitted in partial fulfillment of the requirements

For the award of degree

MASTER OF TECHNOLOGY

in

ELECTRICAL ENGINEERING

by

GUGULOTH SAIKUMAR

EE16B139 (Dual degree)

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY MADRAS

JULY 2021

THESIS CERTIFICATE

ACKNOWLEDGEMENTS

I take pleasure in thanking various people who helped and supported me to carry out this work during execution of the project activities during this pandemic. I am thankful to those who influenced my thinking during the course of study.

I would like to express my sincere thanks to my project guide Dr. K Shanti Swarup, for his support and guidance. His suggestions had been the source of inspiration for me during the conduct of this project.

Finally, most importantly, I wish to express my heartfelt thanks to my family and friends, for being my source of energy.

GUGULOTH SAIKUMAR

ABSTRACT

Smart grids generate the electricity power and transmit the power to different category of customers. One of the basic parts of smart grid systems is advanced metering infrastructure. Smart meter is another basic part of smart grid, which measures the power consumption. The goal of this thesis is first to model the basic functionalities of ami system, then to model a five bus distribution system and show attacker can cause damage to smart grids by changing load which will results in cause of havoc to system.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

FIGURES

TABLES

CHAPTER .1 INTRODUCTION

Cyber physical system is a new technology that integrates cyber systems and physical power systems to high efficiency and performance. CPS is the integration of computational and physical world. CPS applications are used in transportation, robotics, healthcare, manufacture and military etc.

Smart grid is one of the most important applications of CPSs. Smart grids are the electric network that employ advance metering, control and communication technologies to deliver reliable and secure energy supply and enhance operation efficiency for generators and distributers for provide flexible choices for consumers. smart grids are the modern power grids traditional power grids cannot communicate, when compared to smart grids they have advanced communication and computing power . Communication is one of the key features of smart grids. AMI stands for Advanced metering infrastructure is one of the key parts for smart meters.

AMI is a typical cyber physical system which should supervise both cyber and physical attacks. It enables two way communication between utility and smart meters. In general to fix the security for AMI and CPSs is challenging . and one of the reason is CPSs and AMI are complex systems. These thesis mainly address the modelling core functionality of CPS or AMI then we will design security aspects of AMI and specify security related uncertainties of AMI in addition to modeling core functionalities of AMI.

CHAPTER 2 MOTIVATION

In thesis we work on the modelling of AMI related security aspects and in this thesis .we will explain about importance of security for AMI. AMI is a key part of smart grid which enables the bi directional communication between smart grids and utility. For AMI security is the main aspect. If security is not considered it will leads to many problems. The example can be that a hacker can access to smart grid. There are some security concerns for AMI. Integrations within a community and ability to impact consumer's privacy Smart meters are the other part of smart grids, which communicate with AMI.

Smart meters are the digital version of the current power meters. we can see smart meters at customer locations they used measure electrical power usage in meter readings. Smart meters are connected to the smart grid. There are some security threats to smart meters Tampering with device functionality and communication issues between meter and power supplier are examples. In AMI there is more use of cyber sources which may vulnerable to attack. For example, exploited vulnerabilities can result in takeover of devices by attacker. This can lead to crises like city blackouts that can have huge impacts in economy and people's lives. There are few ways to address the security of the AMI like are encryption, physical controls, firewalls, etc. There are also some main challenges of engineering security for CPSs. One of the challenges is when modern CPS wants to

connect to the Internet. By this connection, the worms can be introduced to the system and have impacts on the CPS. Model based security engineering is the solution to handle security of CPSs Motivation for using models is that because CPSs are complex systems, modeling gives more high level of abstraction than coding. This would lead to better security engineering of the system. By modeling, security requirements: confidentiality, integrity, and availability can be considered as early as possible.

These vulnerabilities can have effects on exploiting by attackers or malicious users. Security attacks could also lead to uncertainties in CPSs' functionalities. Therefore, to tackle with these uncertainties, model based security engineering should be focused. It provides a model foundation for reasoning about security-related uncertainties of CPSs, and AMI.

2.2 AIM

In this thesis, we explain the security concerns of smart grids and model the a distribution system and show how attacker will able to cause havoc to the system.

CHAPTER 3 BACKGROUND

In this chapter we will discuss about the key background methodologies like modelling techniques, restricted use case modeling, cyber physical systems, smart grids, and security modeling. Other examples are security of CPSs and security requirements of smart grids and uncertainty.

3.1 Cyber physical systems

CPS is an integration of physical systems with computing devices. Every physical system that is on Network or has internet connection is CPS. They are an embedded system, which monitors Physical environment. In this thesis, we will consider CPSs security issues like Confidentiality, integrity, authenticity, and availability are the most important Security issues. Development of CPS is a model based. That means the models are used for the development of CPS. In this thesis we work with the smart grid. CPS became more popular because of reason is that they are in the field of new research and they have Efficiency and effectiveness. The other reason is that smart grid is a type of cyber physical system which decrease the amount of use of fossil fuels.

Security, resilience, and safety can be a challenge for CPS. Security of cyber physical system is important. In thesis we address the security related uncertainty of Cyber physical systems Smart grid generates electricity power to consumers. There is adversary model for security of CPSs.

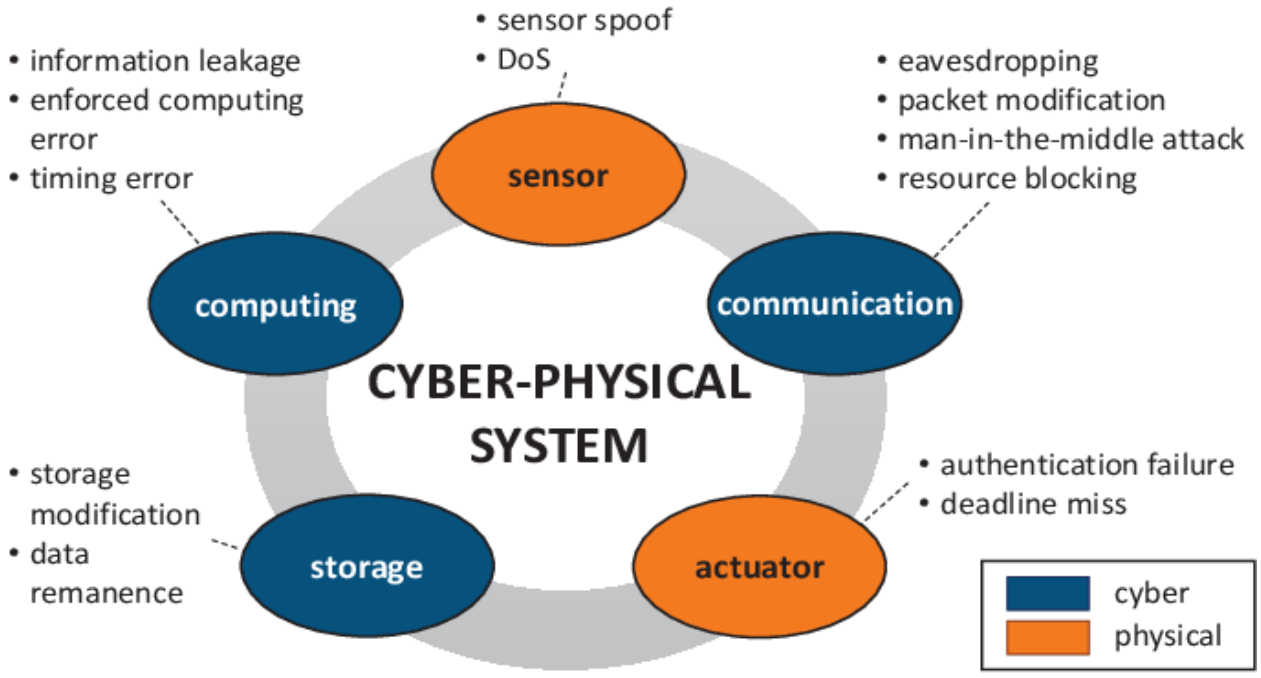


FIG 3.1 CYBER PHYSICAL SYSTEM TOPOLOGY

Cyber physical systems are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. CPS technology would be expected to transform the way people interact with engineered systems like the Internet has transformed the way people interact with information.

3.2 Smart Grids

Smart Grids is one type of CPS. They are power or network electrical systems. They produce Electricity and transmit this power to customers such as factories. Smart grid is one the biggest network which is interconnected throughout the world. Failure in one part of Smart Grid can cause failure to all Smart Grid networks. Researches have shown that demand for smart grid consumption will increases. The reason is that it increases the efficiency of the supply. Consumers tend to use it in an effective manner. The other reason to use smart grids is they use less fossil fuels energies.

The advantages of smart grids is that it can reduce peak demand that they can reduce the peak load demand or optimize it which leads to less

generation of electricity. Other benefit is that smart grids can increase the energy efficiency, because they can make customers more involved in the electricity usage.

However, in addition to the benefits of using SMART grids, there are several weaknesses such as security. Attackers can access smart grid networks and hack some information or they make a few damage to the system. Smart grid security must be considered. If security this is not considered then it will cause damage.

The attacker can hack some information which results in costs and efforts to to bring back to normal stage it also have an economy impact. Reliability will be one of the security challenges for smart grids. The other challenge is the quality of smart grids. The main features of smart grids of the smart grid that it can provide smart meters for the customers. Smart meters can measure the amount of use and price of use. The smart meter provides the security and therefore, the attacker might not access to it.

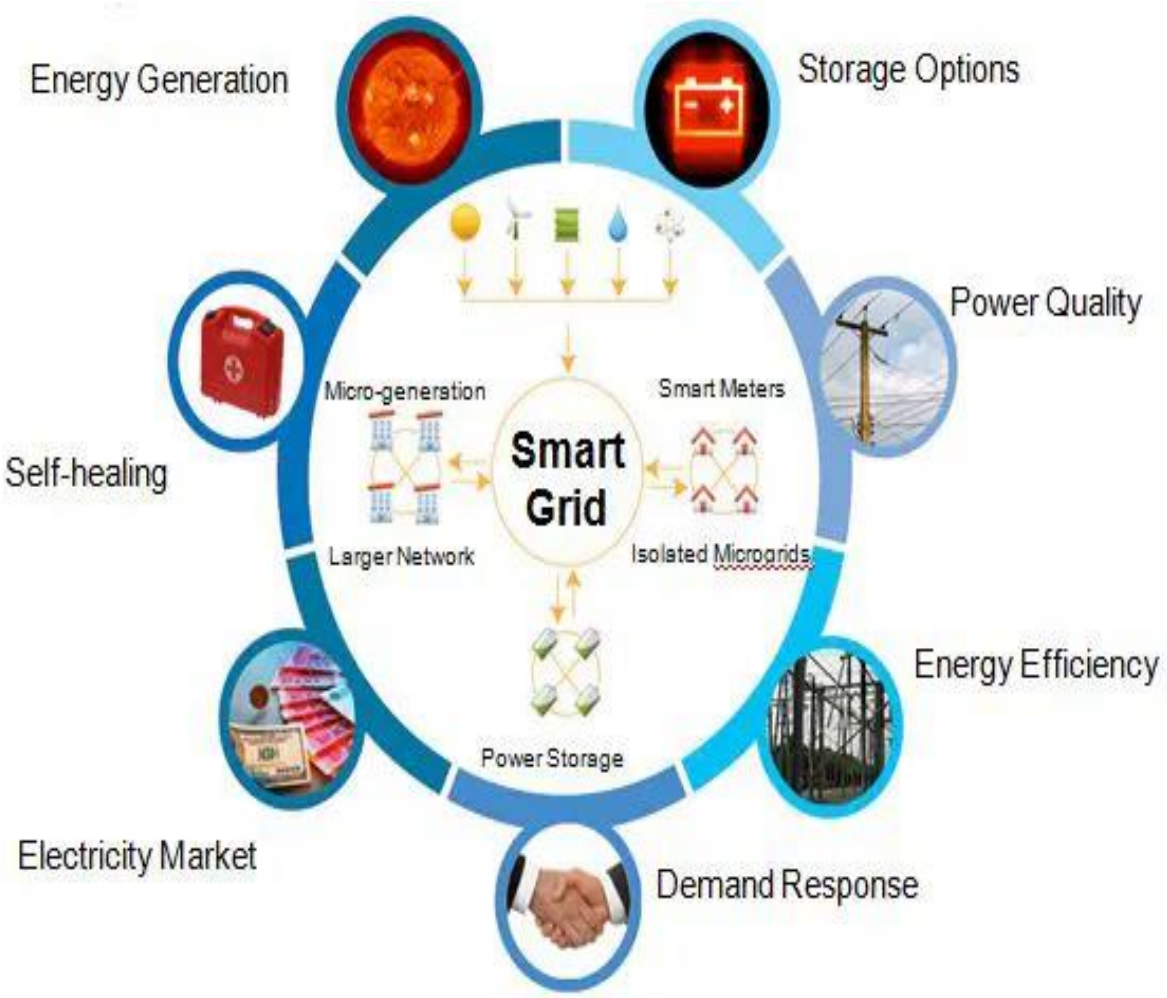


Fig 3.2 SMART GRID ARCHITECTURE

SECURITY MODELLING

Confidentiality, integrity, availability, and accountability are all important aspects of security. These are the required security considerations. For expressing and modelling security needs as well as system functionalities, UML models and UML profiles can be created and used. Because there is a possibility of malicious software that can be harmful to system so that we should secure the system .

We should protect the system from malicious software that can harm it.

3.3 Security of Cyber physical systems

Security of CPSs is significant and it should not come as after thought if it is not considered in the early stage while engineering cyber physical systems if it is not done properly it will be exploited by malicious programs and attack from outside. Important security criteria such as Confidentiality, Integrity, and Availability can be considered. The term confidentiality refers to the fact that the information is private and cannot be accessed by an unauthorized party. The term integrity refers to the fact that data is not changed or modified by an unauthorized party. The term availability refers to the fact that something is Only authorized actors have access to and are aware of the information.

Cyber physical systems can be protected by few methodologies such as encryption, access control, and authentication and security of cyber physical systems also it should consider attacks and hacks from outside as well. The example of cyber physical is smart grids its security concerns will be discussed next.

3.4 Security requirements for smart grids

The safety of smart grids is crucial. Smart grids are devices that generate and transfer electricity to customers such as homes, workplaces, and factories. The smart grid consists of several components, including energy transmission infrastructure, energy distribution infrastructure, and data transmission infrastructure, Data communication network, smart meters, home gateways, network gateways, monitoring modules, and smart appliances. Other components like Decision making modules, energy generators, energy stores, data stores, and electricity market.

Data communication network is the important part of grid. In data communication network different components interact with each other. Because of this interaction it will lead to security risk. There are three different smart grid security objectives or requirements. These are confidentiality, integrity, and availability.

Smart meter is one of the important part of smart grid. It generates data related to energy consumption. The information should be kept private. Customer billing details and forecasts are also included. Energy use information should be kept private. The reason for this is that they deal with sensitive information. Data privacy is the one of the important part of smart grid Customers' personal information, such as identification, energy use, and address, should be kept private.

Smart grids are the which are type of the cyber physical system are likewise subjected to risk. some of the functionalities of AMI can cause vulnerabilities to malicious attack. he other source of uncertainty is security mechanism specification, implementation, and evolution. These will lead to type of uncertainties in the functionality of AMI. An example is incorrect access control can lead to disable physical performance.

TOPOLOGY OF SMART GRID

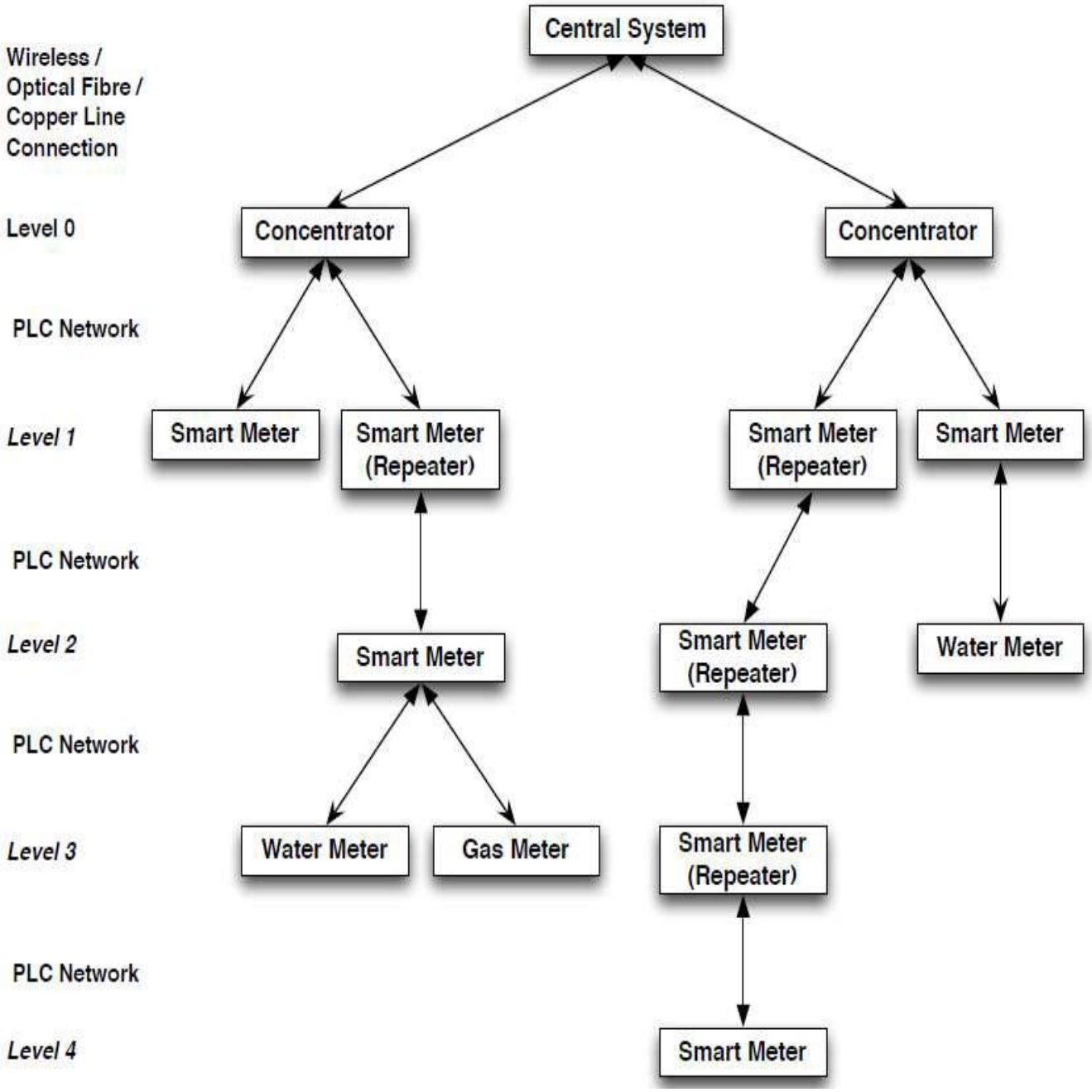


Fig 3.3 topology of smart grid

The topology of a smart grid is described for the purposes of evaluating, simulating, and developing smart grid infrastructures. Smart grid topology consists of several components such as smart meters, repeaters, and other smart meters. Due to the possibility of interference, these repeaters are used to connect smart meters to concentrators since there might be the distance in the way smart grids to concentrators which control smart grids. At the top of the topology is central system, which stores the consumption data. There are water meters, gas meters, or heat meters in the topology. Smart meters are connected to concentrators, and concentrators are connected to smart meters. Customers' water consumption is measured using water meters. Customers' gas consumption is measured using gas or heat meters. They aren't connected to concentrators directly.

The topology is represented by a tree with subtrees. Smart meters are connected eit her directly to concentrators or indirectly via repeaters due to noise and distance Concentrators are the root node of subtrees. The central system is the root of the whole topology tree. Smart meters and the repeaters are the leaves of the topology tree.

Topology can be measured in a variety of ways. The number of smart meters in the topology and the average number of them are two instances.

The path length from a smart meter to the concentrator is another measurement. The amount of hops is what it's called. Another type of measuring is the physical distance between smart meters and concentrators. Because the smart grid topology is a communication topology, security is taken into account for the communication element when it comes to security and security modelling. Another security consideration is that communication topologies can be built using power lines PLC (programmable logic controller network. Wireless technology is also used to connect the subtrees in the smart grid architecture. This implies that security modelling should be used to represent the relationships between various components of the topological subtree and tree.

One of the security vulnerabilities addressed by the reasoning engine is "malicious shutdown commands." The reasoning engine is in charge of monitoring and detecting sections in the smart grid that are shut down remotely as a result of malicious activities. The reasoning engine then adds these harmful attempts to a blacklist, preventing them from spreading to other locations. For detecting entities that are shut do, the greedy approach is utilized. Which is shutdown.

3.5 METHODOLOGY

In this thesis we use UML as the primary technique to model the Cyber physical systems, security and security related uncertainties of cyber physical systems and we model a five bus system and show how attacker can able to control the load according to his desire and cause havoc to the system.

STRUCTURE OF ADVANCE METERING INFRASTRUCTURE

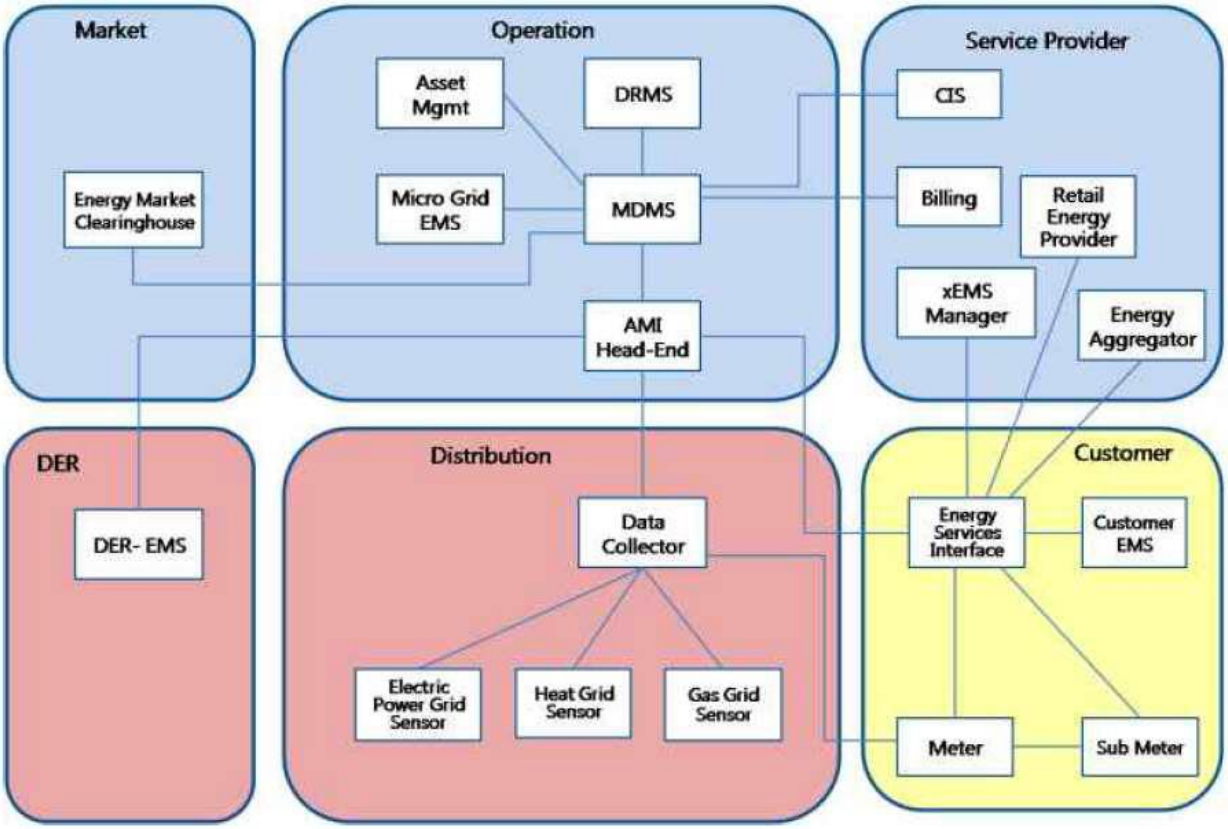


Fig 3.3 Reference model for advance metering infrastructure

There are four subsections in this section. We present general definitions of AMI head-end, smart meters, Customer Information System (CIS), and AMI head-end main features in these subsections, respectively. In section, we go through the smart grid's security design. This section is broken into three subsections: authentication, authorization, and finally encryption and decryption.

AMI head end

AMI head-end is the back office system that controls and manages the overall advanced metering infrastructure system The AMI head-end is a smart grid component that establishes two-way communication with smart meters. The AMI head-end is located on the smart grid's server side. Smart meters, on the other hand, are located on the client side of the smart grid. As a result, the AMI headend and the smart meter are on opposite sides. That is the reason we separated AMI head-end and smart meter in UML design of this thesis. Metering services including periodic meter reading, on-demand meter reading, and remote meter connect/disconnect are the major functions of the AMI head-end. Meter reading and remote meter connect/disconnect.

We will design these functionalities by using UML in the following sections. We will specify them by use case diagrams.

3.6 SMART METERS

Smart meters in smart grids are used for measuring the electricity consumption of consumer Between the consumer and the utility, there is automatic and bidirectional communication. Electricity usage can be read by smart meters both locally and remotely. Smart meters have the advantage of informing users about how much electricity they are using, as well as how often and when they are using it. Another advantage is that smart meters enable consumers to use electricity more efficiently and effectively. Smart meters provide users with information about their electricity usage. Smart meters give users more control over and management of the system. Smart meters can provide them with data. Then they will be able to manage the information.

Core Functionalities of Ami Head-End

Periodic Meter Reading

Periodic meter reading is one of the core functionalities of AMI head end. Which we will address in this thesis by modelling. The smart meter monitors energy power use at predetermined periods in periodic meter reading. In our situation, the intervals are 15 minutes. It means that every 15 minutes, the electricity use is recorded. The smart meter will then gather data from the meter, which in our case is energy power consumption every four hours. smart meter will send the transfer the data from the meter to the AMI head-end Finally, this data will send to the customer for billing and payment purpose.

On-Demand Meter Reading

Another important feature of the AMI head-end is on-demand meter reading. It's similar to taking a meter reading on a regular basis. The difference is in periodic meter reading, in which the meter read data or electricity power consumption is communicated to the AMI head-end and the client on a regular basis. On-demand meter reading, on the other hand, obtains meter read data depending on demand and request on a predetermined date and time. AMI head-end receives an on-demand meter read request message from CIS. This communication is sent from the AMI

headend to the smart meter. The meter read data will be retrieved by the smart meter and sent to the AMI headend. At the completion of the process, the AMI head-end will provide this information to CIS.

Remote Meter Connect/Disconnect

The remote meter connect/disconnect capabilities of the AMI head-end is another feature that we will discuss in our thesis. Smart meters will be linked and disconnected for various causes in this feature. For example, a smart meter can be turned off due to non-payment. The smart meter will be disconnected if the consumer fails to pay for his or her consumption. CIS transmits a remote meter connect/disconnect message to the AMI head-end during remote meter connect/disconnect. This communication is sent from the AMI headend to the smart meter. The smart meter will then take action in response to the message it receives. If the message says "remote meter connect," the smart meter will turn off the meter switch and connect remotely. Otherwise If the message is for remote meter disconnect, the smart meter will open the meter switch and disconnect the meters remotely. The smart meter will then send a verification or acknowledgment message to the AMI head-end in both circumstances to show that it is connected or disconnected. At the completion of the process, the AMI head-end will transmit this verification message to CIS.

Security design of smart grid

In this we model security aspects of smart grid and we cover security requirements of AMI system. There are some security requirements for AMI system. These requirements are Confidentiality, Integrity, Availability and Accountability

In the thesis, we offer several security approaches for developing smart grid systems. The sub-sections that follow detail these mechanisms. They are the security procedures of authentication, authorization, encryption, and decryption. For modelling the security aspects, we employ UML diagrams as an approach.

Table 3.1 Use cases of AMI Head-End

Name	Description	Actor/Subsystem
AMI Head-End	AMI head-end is the back office in the smart grid. It controls the advanced metering infrastructure.	Subsystem
Smart Meter Controller	Smart meter controller is part of AMI head-end. Since there are many smart meters in the system, smart meter controller is the one to handle and manage all the smart meters. It deals with smart meters.	Actor
Session Manager	Session manager is used to manage sessions. It performs tasks such as create session and look up session.	Actor
Session	Session is used in authorization process. It acts as a policy decision point. It has the access rights of smart meter. When smart meter controller sends authorization request to session, it checks the access rights of smart meter and returns the authorization decision to smart meter controller.	Actor

Smart Meter	Smart meter is used for measuring the electricity consumption of consumer. Smart meter communicates with AMI head-end.	Actor

AMI-Head-End's Initialization of Use Case Diagram

SUMMARY

From the AMI head-end side, this is the initial use case diagram. In this use case diagram, there is only one use case and one actor. Initialization is the use case, and AMI head-end is the actor. This use case serves as a prerequisite for the use cases that follow. The AMI head-end will be initialized in this use scenario. It signifies that there are some procedures to take in order to get the AMI head-end ready to listen connection from smart meters.

DESCRIPTION OF USE CASE

As previously said, this use case diagram only has one use case, which is the initialization use case. AMI head-end is the actor in charge of carrying out this use case. There are a few modest steps inside the initialization use case that must be completed in order for the AMI head-end to be initialized. The AMI headend must first generate a server socket. The server socket's job is to listen to the network and wait for responses from smart meters. We don't need to show server socket in the use case diagram because it's part of AMI head-end. The configured port number is used to build a server socket.

There are two conditions that must be met when creating a server socket. The server socket can be successfully created or the creation of a server socket may fail. If it is successfully generated, the server socket will be ready to accept connection requests from the smart meter. After that, it prepares the environment for establishing a two-way connection between the AMI headend and the smart meter. If the server socket creation fails, the AMI head-end will display an error message. The server socket should then be created again.

THE USE CASE DIAGRAM

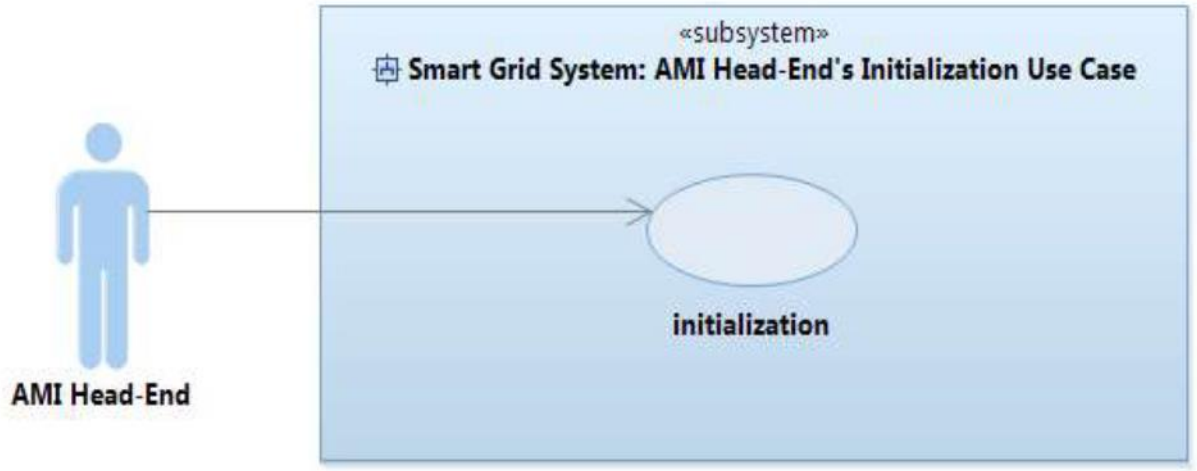


Fig **3.4** AMI Head-End's Initialization Use Case Diagram

AMI Head-End's Initialization	
Use Case ID	UC Initialization

Use Case Name	Initialization	
Description	This use case shows how AMI Head-end is initialized. For example, this use case should contain all the steps to make AMI head-end ready to listen to connection requests from smart meters.	
Precondition	AMI head-end is configured.	
Primary Actor	AMI head-end	
Secondary Actors	None	
Dependencies	None	
Basic Flow	Steps:	
	1	AMI head-end creates a server socket with the configured port number.
	2	IF server socket is created successfully THEN DO
	3	The server socket is waiting for connection from smart meters.
	4	A smart meter connects to the sever socket, which returns a client socket to that smart meter.
	5	AMI head-end creates a concurrent process to handle the establish connection (UC Establish Two-way Connection) to that smart meter MEANWHILE AMI head-end continues to wait for

		connection from smart meters. UNTIL server socket is closed.	
	Post Condition	AMI head-end continues waiting for connection requests from smart meter.	
Specific Alternative Flow	RFS Basic Flow 2		
	Steps:		
	1	ELSEIF server socket is not created successfully because the port is in use THEN	
	2	AMI head-end shows an error message.	
	3	AMI head-end is reconfigured with an unused port number.	
	4	RESUME Step 1	
	5	ENDIF	
	Post Condition	AMI head-end is reconfigured.	

AMI Head-End Establishes Connection with Smart Meter Use Case

Summary

This use case diagram has three use cases. In this diagram, the major use case is "Establish Two-way Connection." Other use cases that are included in the main use case are "Receiving Package from Smart Meter" and "Sending Package to Smart Meter." AMI head-end and smart meter are the actors.

Description of Use Cases

Following the initialization of the AMI head-end, the following step is to link the AMI head-end to the smart meter. Between the AMI headend and the smart meter, there is a two-way connection. There are a few processes involved in establishing connection. First, the AMI head-end acknowledges the smart meter's connection request. The connected acknowledgment message is then delivered by AMI head-end to smart meter, indicating that AMI head-end has accepted the connection request sent by smart meter.

The Use Case Diagram

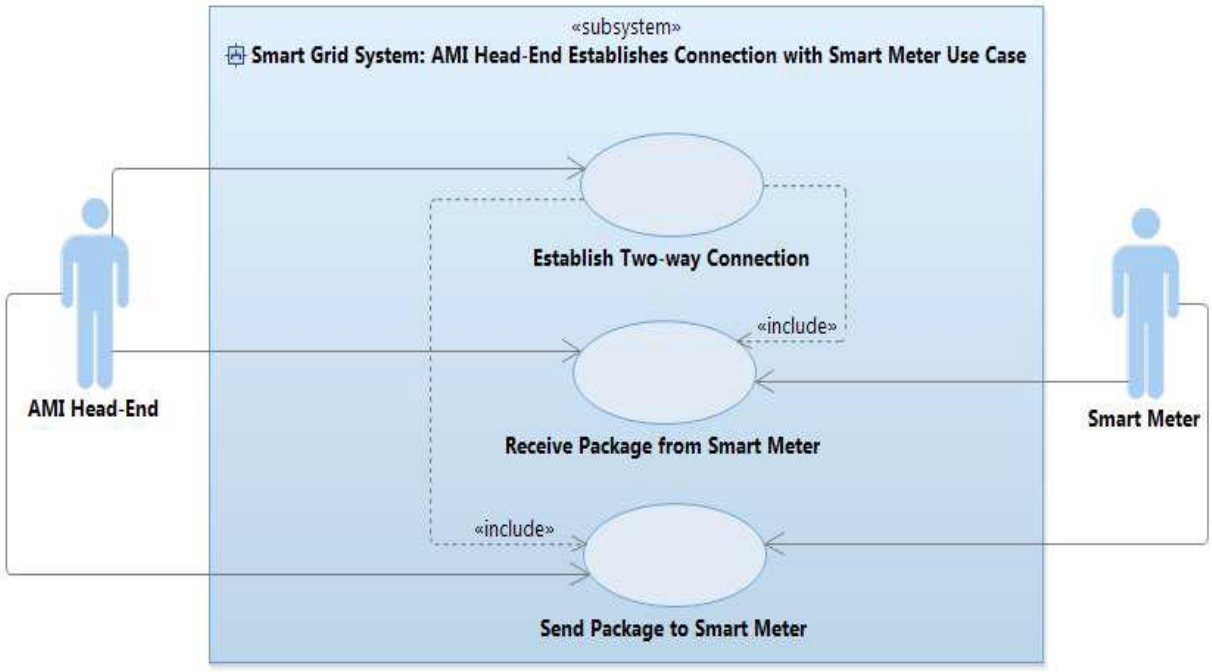


Fig 3.5 AMI Head-End Establishes Connection with Smart Meter Use Case Diagram

Table 3.2 AMI Head-End Establishes Connection with Smart Meter Use Case

AMI Head-End Establishes Connection with Smart Meter	
Use Case ID	UC Establish Two-way Connection
Use Case Name	Establish Two-way Connection
Description	This is the first step in registration process of smart meter. In this step

	AMI head-end establishes connection with smart meter.	
Precondition	A client socket for the connection to the requesting meter has been created.	
Primary Actor	AMI head-end	
Secondary Actors	Smart Meter	
Dependencies	INCLUDE USE CASE Receiving Package from Smart Meter INCLUDE USE CASE Sending Package to Smart Meter	
Basic Flow	Steps:	
	1	A new concurrent process uses the client socket (i.e., the connection to the smart meter) for constantly waiting to receive packages sent from smart meter (UC_ReceivingPackageFromMeter) MEANWHILE the client socket can also be used for sending packages from AMI head-end to smart meter.
	2	The client socket is used for sending a package with connected acknowledgment message to smart meter (UC_SendingPackageToMeter).

	Post Condition	There is a two-way connection between AMI head-end and smart meter, i.e., head-end side is ready to receive packages from smart meter as well as to send packages from head-end to smart meter.

Receiving Package from Smart Meter Use Case

Summary

This use case is a general use case for receiving all kinds of packages from smart meter. The main use case in this use case diagram is “Receive Package from Smart Meter”. This use case includes “Decrypt Package”, “Response to Smart Meter” and “Send Package to Smart Meter” use cases. The actors are smart meter controller and smart meter.

Description of Use cases

AMI head-end waits for receiving package from smart meter. Then smart meter controller, which is part of AMI head-end will receive a package from smart meter. After that, smart meter controller will verify the received package from smart meter and will decrypt the received package. If the package is from expected smart meter, then it will process the package. Otherwise, it will send an error message to smart meter.

Use case diagram

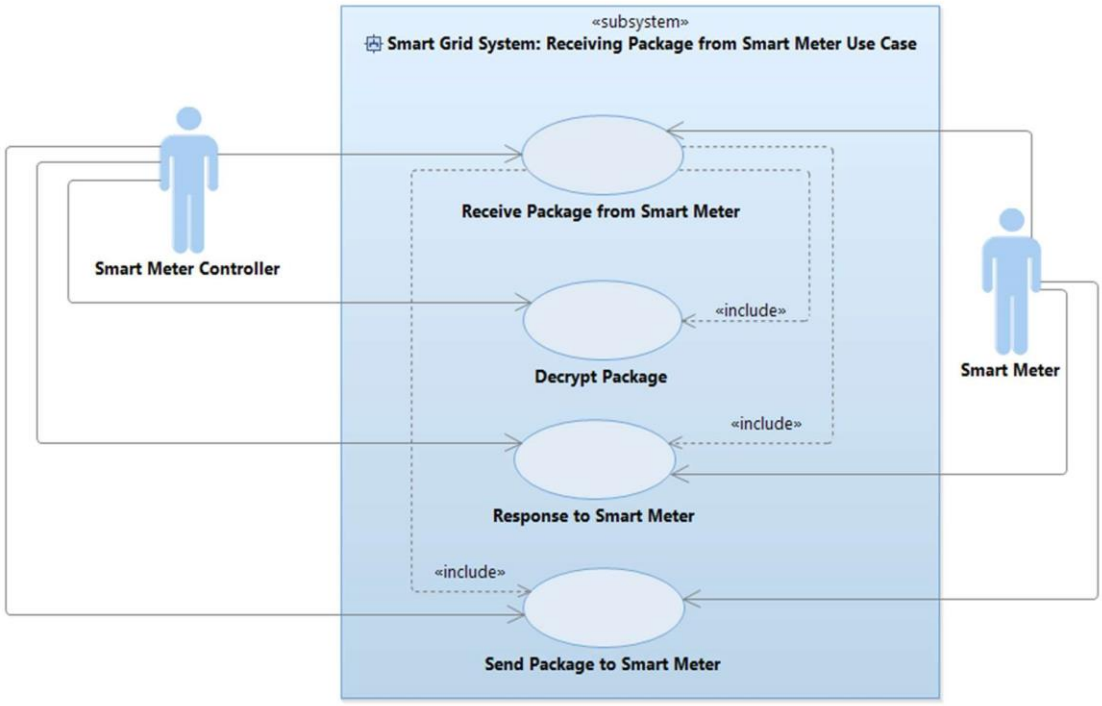


Fig 3.6 Receiving Package from Smart Meter Use Case Diagram

Table 3.2 Receiving package from smart meter

Receiving package from smart meter	
Use Case ID	UC_ ReceivingPackageFromMeter
Use Case Name	Receive Package from Smart Meter
Description	This is a general use case for specifying how AMI head-end receives packages from smart meter.
Precondition	A client socket for the connection to the requesting meter has been created.
Primary Actor	Smart meter controller
Secondary Actors	Smart Meter

Dependencies	INCLUDE USE CASE Decrypt Package INCLUDE USE CASE Response to Smart Meter INCLUDE USE CASE Send Package to Smart Meter		
Basic Flow	Steps:		
	1	DO	
	2	AMI head-end is waiting to receive package from the smart meter.	
	3	Smart meter controller receives a package from the smart meter.	
	4	IF smart meter controller, which is part of AMI head-end verifies the digital signature and decrypts the received package from the smart meter (UC_DecryptPackage) THEN	
	5	Smart meter controller creates a new concurrent process (thread) to process the decrypted package (UC_ResponseToMeter) MEANWHILE AMI head-end continues waiting for receiving packages.	
	6	UNTIL the client socket is closed.	
	Post Condition	The package is received from smart meter to head-end.	
Specific Alternative Flow	RFS Basic Flow Step 3		
	Steps:		
	1	ELSEIF smart meter controller does not verify the digital signature or decrypt the received package from the smart meter THEN	
	2	Smart meter controller creates a new concurrent process (thread) to send a package with error message/code to the smart meter (see UC_SendPackageToMeter).	
	3	ABORT	
	4	ENDIF	
	Post Condition	A package with error message/code is sent to the meter.	

Sending Package to Smart Meter Use Case

Summary

This is a use case for sending package from smart meter to AMI head-end. There are two use cases in this use case diagram. First use case is “Send Package to Smart Meter”. The

other use case is “Encrypt Package”. This use case is included from the first use case. The actors are smart meter controller and smart meter.

Description of Use Cases

AMI head-end wants to send a package to smart meter. Smart meter controller creates a data package and sends a package to smart meter. Before sending a package to smart meter, smart meter controller first should encrypt and sign the package for the security purposes. Then smart meter controller will send the package to smart meter.

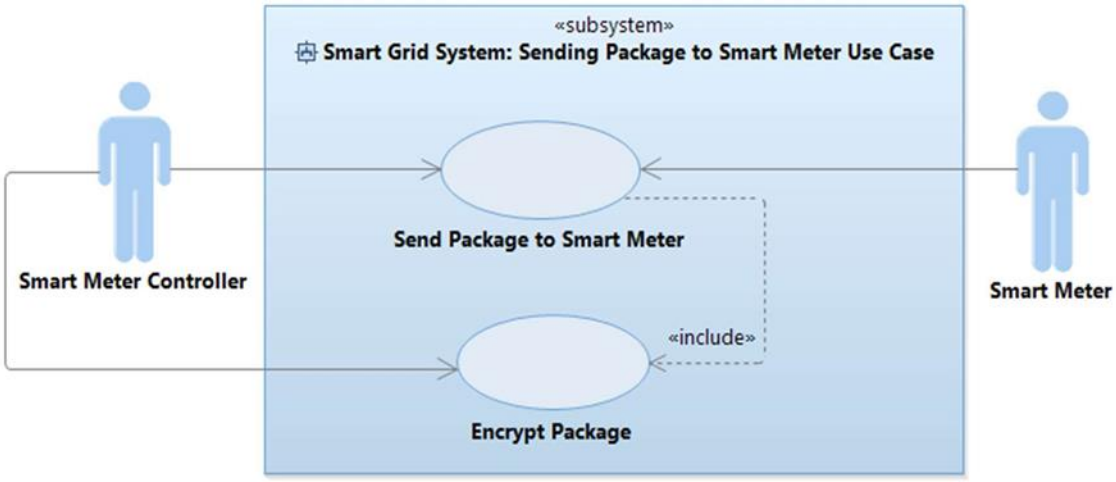


Fig 3.7 sending package to smart meter

Table 3.3 sending package to smart meter

Sending package to smart meter	
Use Case ID	UC_ Sending Package To Meter
Use Case Name	Send Package to Smart Meter
Description	This is a general use case for specifying how AMI head-end sends packages to smart meter.
Precondition	A client socket for the connection to the requesting meter has been created.
Primary Actor	Smart meter controller

Secondary Actors	Smart meter	
Dependencies	INCLUDE USE CASE Encrypt Package	
Basic Flow	Steps:	
	1	Smart meter controller creates a package for sending to the smart meter.
	2	IF smart meter controller encrypts and signs the package THEN
	3	Smart meter controller sends the package to the smart meter via client socket.
	Post Condition	The package is sent to the smart meter.
Specific Alternative Flow	RFS Basic Flow 2	
	Steps:	
	1	ELSEIF smart meter controller does not sign the package THEN
	2	Smart meter controller creates a new concurrent process (thread) to send a package with error message/code to the smart meter .
	3	ABORT
	4	ENDIF
	Post Condition	A package with error message/code is sent to the meter.

Response to Smart Meter Use Case

Response to smart meter use case is a general use case to show how AMI head-end will respond to smart meter after it received the package from smart meter. Depending the package code, AMI headend will respond to smart meter differently. There are different use cases in this use case diagram. The main use case is “Response to Smart Meter”. Other use cases are included from this use case.

Description of Use Cases

The main use case in this use case diagram is “Response to Smart Meter”. AMI head-end after receiving the packages will process the packages depending on the package code

and will respond to smart meter. For example, if the package code is for the authentication of smart meter, then AMI headend will authenticate the smart meter, otherwise it will act differently. For example, if the package code is periodic meter reading from smart meter, then AMI head-end will process the meter read data

The Use Case Diagram

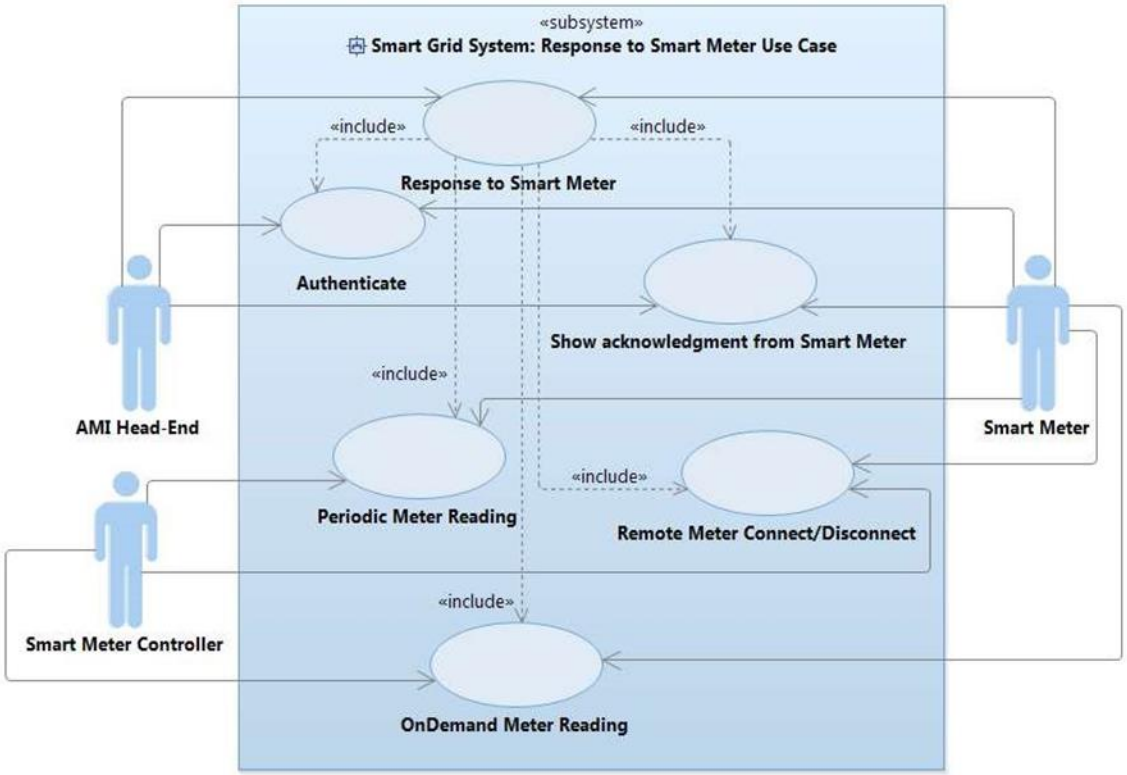


Fig 3.8 Response to Smart Meter Use Case Diagram

Table 3.3 response to smart meter

Response to smart meter	
Use Case ID	UC_ResponseToMeter
Use Case Name	Response to Smart Meter

Description	This is a general use case for specifying how head-end side processes a received package from smart meter.	
Precondition	A package from meter has been received and decrypted successfully.	
Primary Actor	Smart meter controller	
Secondary Actors	AMI head-end, Smart Meter	
Dependencies	INCLUDE USE CASE Authenticate INCLUDE USE CASE Show Acknowledgment from Smart Meter INCLUDE USE CASE Periodic Meter reading INCLUDE USE CASE Remote Meter Connect/Disconnect INCLUDE USE CASE On-Demand Meter Reading	
Basic Flow	Steps:	
	1	Smart meter controller reads the decrypted package to check the package code.

2	IF the package code is for the authentication of smart meter THEN
3	AMI head-end authenticates the smart meter. (UC_Authentication).
4	ELSEIF the package code is the ACK message of meter that it is configured successfully THEN
5	AMI head-end shows the message. (UC_ShowACKfromMeter)
6	ELSEIF the package code is the Periodic Meter Readings from meter THEN
7	Smart meter controller processes the Meter Readings data. (UC_PeriodicMeterReading)
8	ELSEIF the package code is internal meter switch verification message from meter THEN
9	Smart meter controller processes the internal meter switch verification message.(UC_RemoteMeterConnect/Disconnect)
10	ELSEIF the package code is on-demand meter read data from smart meter THEN
11	Smart meter controller processes the on-demand meter read data. (UC_On-DemandMeterReading)
12	ELSEIF the package code is unknown to the headend side THEN
13	AMI head-end sends to smart meter a package with the error message that the package code is unknown (UC_SendPacakgeToMeter).
14	MMB shows the error message.
15	ENDIF
Post Condition	The package from meter has been processed, i.e., a response from headend side is sent back to smart meter.

Authentication Use case

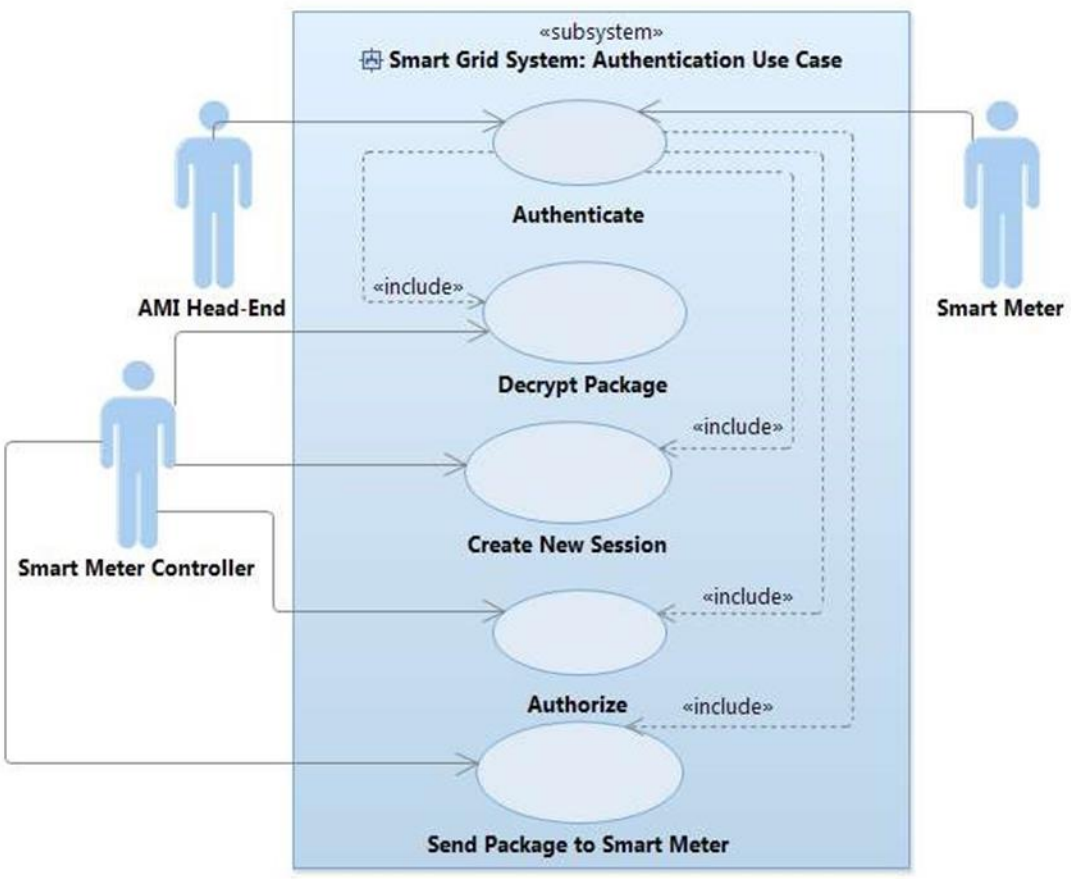
Summary

Authenticate use case is a security related use case for sending or receiving packages to/from smart meter. This use case includes different use cases such as “Decrypt Package”, “Crete New Session”, “Authorize”, and “Send Package to Smart Meter”.

Description of Use Cases

When the connection is established between smart meter and AMI head-end, smart meter will send its credentials (id and password) to be authenticated by AMI head-end. In the process of smart meter authentication, after smart meter sends its credentials to AMI head-end, smart meter controller verifies smart meter's credentials. If the verification process is successful, AMI head-end authenticates smart meter. Then smart meter controller creates a session and sends session id to the smart meter. Smart meter saves this session id to use it in later processes. If the authentication process is not successful, smart meter controller sends the error message to smart meter.

Fig 3.9 The Use Case Diagram



Periodic Meter Reading Use Case

Summary

There is one main and high-level use case in this use case diagram, which is called “Periodic Meter Reading”. This use case includes other use cases such as “Authenticate”, “Receive Package from Smart Meter” and “Authorize” use cases. The primary actor in this use case diagram is AMI head-end. The secondary actors are smart meter controller and smart meter.

Description of Use Cases

Periodic meter reading is the high-level use case. In the process of periodic meter reading from the AMI head-end side, smart meter controller receives a periodic meter read data from smart meter. However, before receiving the meter read data, AMI head-end first should check if the smart meter has already been authenticated by AMI head-end or not. If the session is active, it means smart meter has been authenticated by AMI head-end. In this cases, smart meter controller can receive the package from smart meter. Otherwise, if the session is timed-out, smart meter needs to be re-authenticated by AMI head-end. Therefore, in this case after smart meter has been authenticated again by AMI headend, smart meter controller can receive the meter read data. After receiving meter read data, it should also be authorized.

The use case diagram

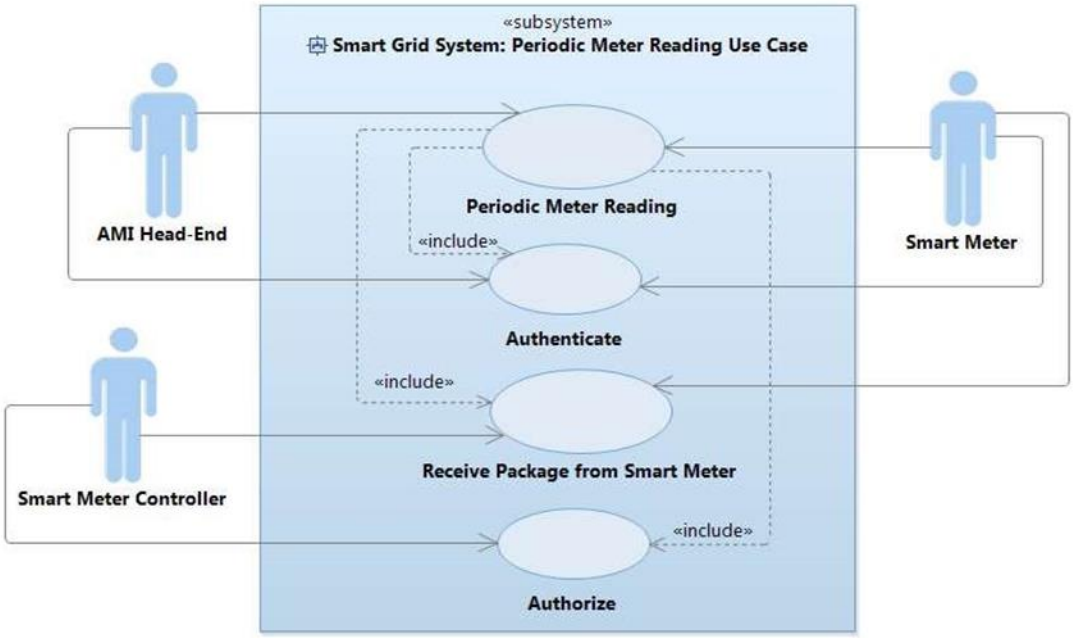


Fig 3.10 Periodic Meter Reading Use Case diagram

Table 3.4 Periodic meter reading

Periodic Meter Reading	
Use Case ID	UC_PeriodicMeterReading
Use Case Name	Periodic Meter Reading
Description	Periodic meter reading is a high-level use case. After the record service, records the 15 minutes electrical usage data, meter metrology board collects the meter read data every 4 hours. Then NIC packages meter read data. NIC sends the meter read data to AMI head-end.
Precondition	Smart meter has sent the periodic meter read data to AMI head-end.
Primary Actor	AMI head-end
Secondary Actors	Smart meter controller, Smart meter
Dependencies	INCLUDE USE CASE Authenticate INCLUDE USE CASE Receive Package from Smart Meter INCLUDE USE CASE Authorize
Basic Flow	Steps:

	1	In order for AMI head-end to receive the package including meter read data from smart meter, AMI head-end needs to check if the smart meter has already authenticated by AMI head-end or if the session is still active or it is timed out. (UC_Authentication)	
	2	IF the session is active THEN	
	3	Smart meter controller receives the encrypted meter read data from smart meter. (UC_ReceivingPackagefromMeter)	
	4	AMI head-end authorizes smart meter. (UC_Authorization)	
	Post Condition	AMI head-end receives the meter read data.	
Specific Alternative Flow	RFS Basic Flow 2		
	Steps:		
	1	ELSEIF the session is timed out THEN	
	2	AMI head-end re-authenticates smart meter by re-using authenticate use case.	
	3	RESUME STEP 3	
	4	ENDIF	
	Post Condition	-	

Remote Meter Connect/Disconnect Use Case

Summary

There is one main and high-level use case in this use case diagram, which is called “Remote Meter Connect/Disconnect” use case. All other use cases in this use case diagram are reused by this main use case. These use cases are “Send Package to Smart Meter”, “Receive Package from Smart Meter”, “Authorize” and “Authenticate” use cases. AMI head-end is the primary actor.
Smart Description of Use Cases

In the process of remote meter connect/disconnect, first CIS sends remote meter connect/disconnect request message to AMI head-end. Then head-end needs to send remote meter connect/disconnect message to smart meter. However, before sending the message, smart

meter should be already authenticated by AMI head-end. Therefore, AMI head-end checks the session status. If the session is active, smart meter controller sends the remote meter connect/disconnect message to smart meter. Then smart meter controller receives the closed/opened internal meter switch verification message from smart meter. This package is authorized. If the session is timed out, AMI head-end reauthenticates the smart meter. AMI head-end sends the encrypted message to CIS at the end meter controller and smart meter are the secondary actors in this use case diagram.

Use case diagram

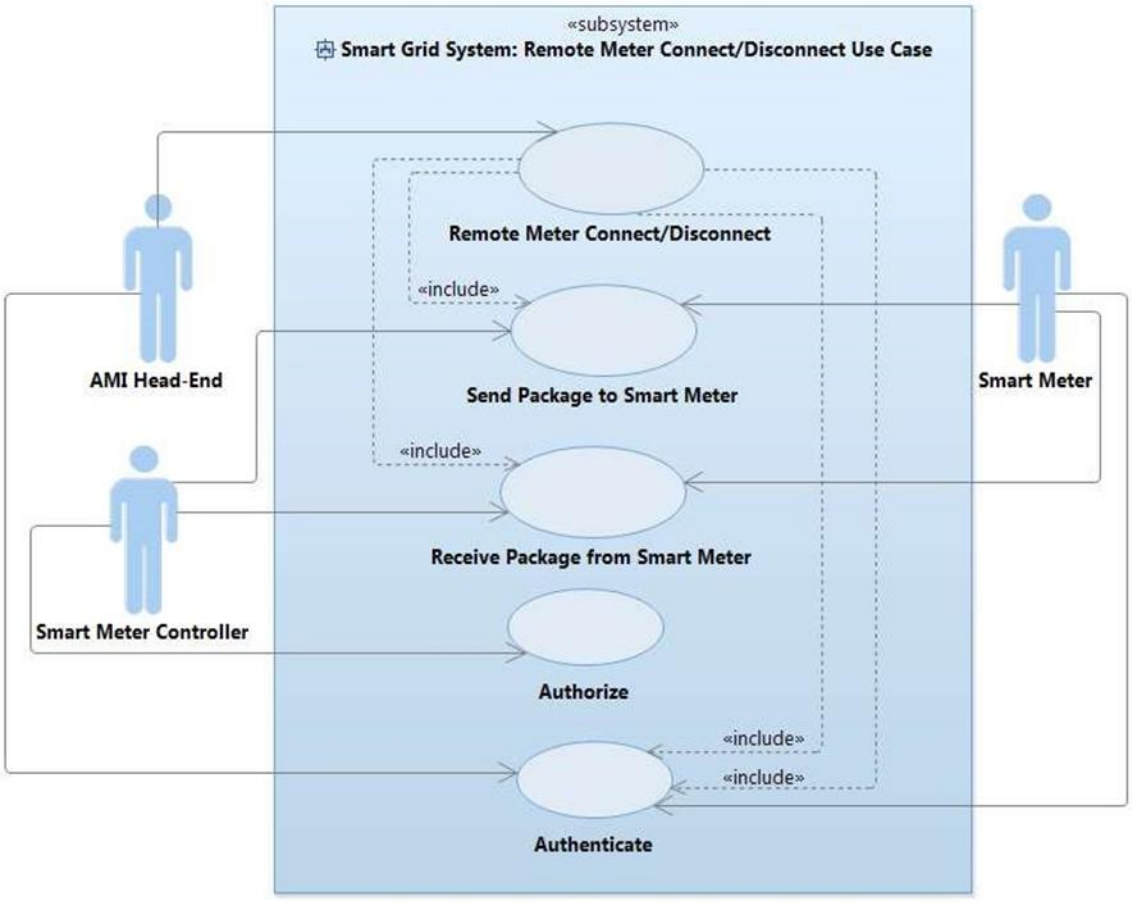


Fig 3.11Remote Meter Connect/Disconnect Use Case

On-Demand Meter Reading Use case

Summary

"On-Demand Meter Reading" use case includes "Send Package to Smart Meter", "Authorize", and "Authenticate" use cases. The primary actor is AMI head-end and the secondary actors are smart meter controller and smart meter in this use case diagram.

Description of Use Cases

In the process of on-demand meter reading, first CIS sends on-demand meter read request message to AMI head-end. AMI head-end will send this message to smart meter. However, since this message is sensitive, AMI head-end needs to authenticate smart meter. Therefore, AMI head-end checks the session status. If the session is active, then there is no need to authentication. Smart meter controller sends the on-demand meter read request message to NIC, which is a part of smart meter. NIC sends on-demand meter read data to smart meter controller. The meter read data is authorized. At the end, AMI head-end sends the on-demand meter read data to CIS. On the other hand, if the session is timedout, it means there is a need for re-authentication process. Therefore, AMI head-end will reauthenticate the smart meter.

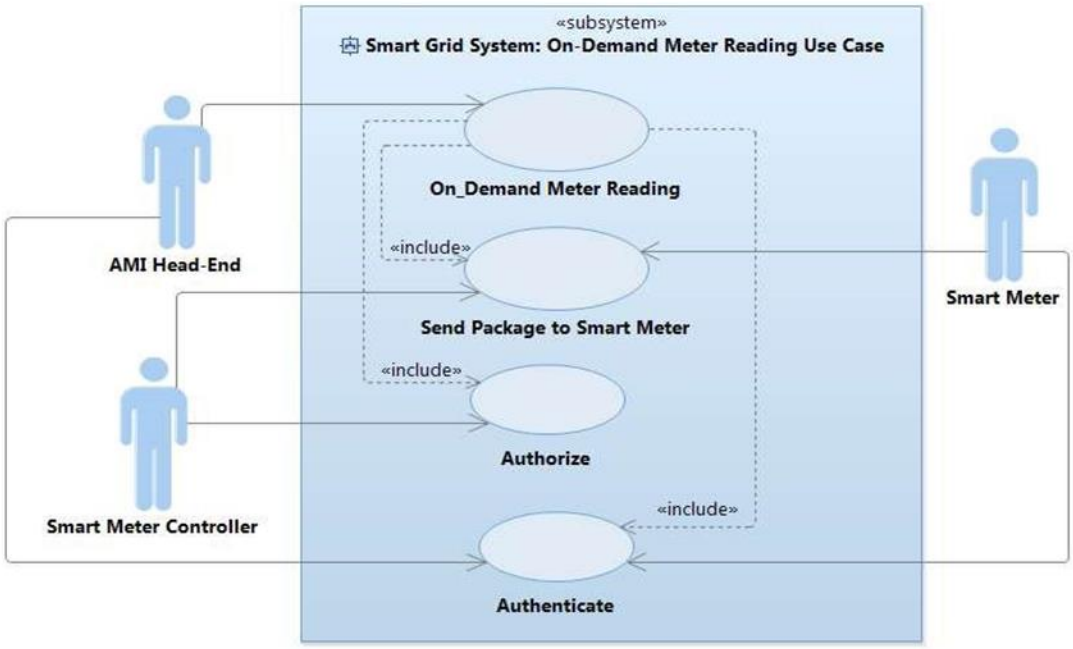


Fig 3.12 On-Demand Meter Reading Use case

Use cases of Smart Meter

Table3.5 Actors for Smart meter use case

Name	Description	Actor/Subsystem
Smart Meter	Smart meter is used for measuring the electricity consumption of consumer. Smart meter communicates with AMI head-end. Smart meter consists of some small parts such as Meter Metrology Board (MMB), NIC, and Internal Meter Switch.	Actor
Meter Metrology Board	Meter Metrology Board is a part of smart meter, which is responsible for performing some operations or functions such as recording the meter's electrical usage data in formatted table, controlling the internal meter switch to close/open, and retrieving meter read data in formatted table.	Actor

NIC	NIC is the other part of smart meter, which is responsible for transmitting or sending data from Meter Metrology Board to AMI head-end or from AMI headend to Meter Metrology Board.	Actor
Internal Meter Switch	Internal Meter Switch is a part of smart meter. It executes the RCD (remote connect/disconnect) command to close or open the meter switch. When there is a connect command, it closes the meter switch. Otherwise, when there is a disconnect command it opens the meter switch.	Actor
AMI Head-End	AMI head-end is the back office in the smart grid. It controls the advanced metering infrastructure.	Subsystem

Recording the Meter's Electrical Usage Data Use Case Diagram

Summary

The use case in this use case diagram is called "Record the Meter's Electrical Usage Data". This use case is a sub-use case of "Periodic Meter Reading" use case. The actor to perform this use case is meter metrology board.

Description of Use Cases

In this use case, meter metrology board creates the record service. The, record service will record the meter's electrical usage data for 15 minutes interval.

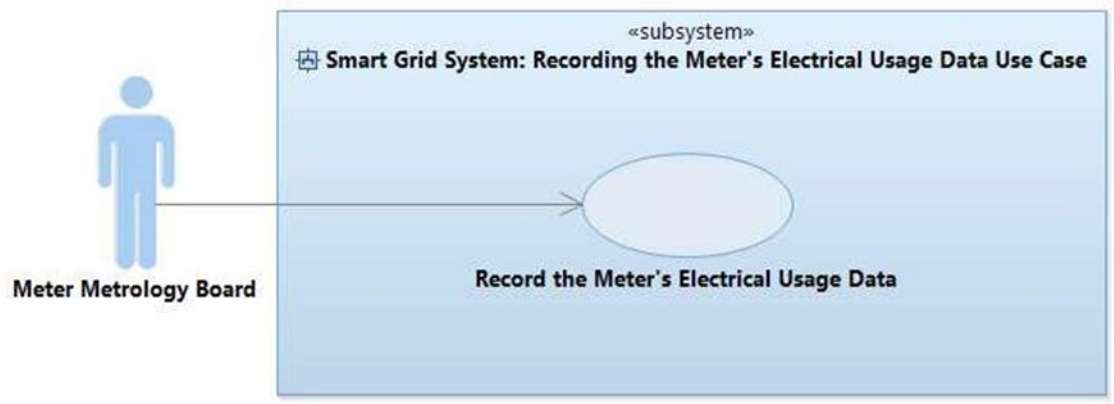


Fig 3.13 Recording the Meter's Electrical Usage Data Use case Diagram

Remote Meter Connect/Disconnect Use Case Diagram

Summary

In this use case, the smart meter can be connected or disconnected for applying some changes in the system. For example, if the consumer does not pay the cost, the smart meter is disconnected. The main and high-level use case in this use case diagram is "Remote Meter Connect/Disconnect". This use case includes "Authenticate", "Receive Package from AMI Head-End", "Authorize", "Encrypt Package", and "Send Package to AMI Head-End" use cases. The primary actor is NIC. The secondary actors are meter metrology board, internal meter switch and AMI head-end.

Description of use cases

The main use case in this use case diagram is "Remote meter Connect/Disconnect". NIC receives remote meter connect/disconnect message sent by AMI head-end. Then Meter Metrology Board controls Internal Meter Switch. Internal Meter Switch, which is part of smart meter, executes the RCD command to close/open the meter switch. Meter Metrology Board creates Internal Meter

Switch Verification message. Meter metrology board encrypts the message. Then NIC sends the encrypted Internal Meter Switch Verification message to AMI head-end.

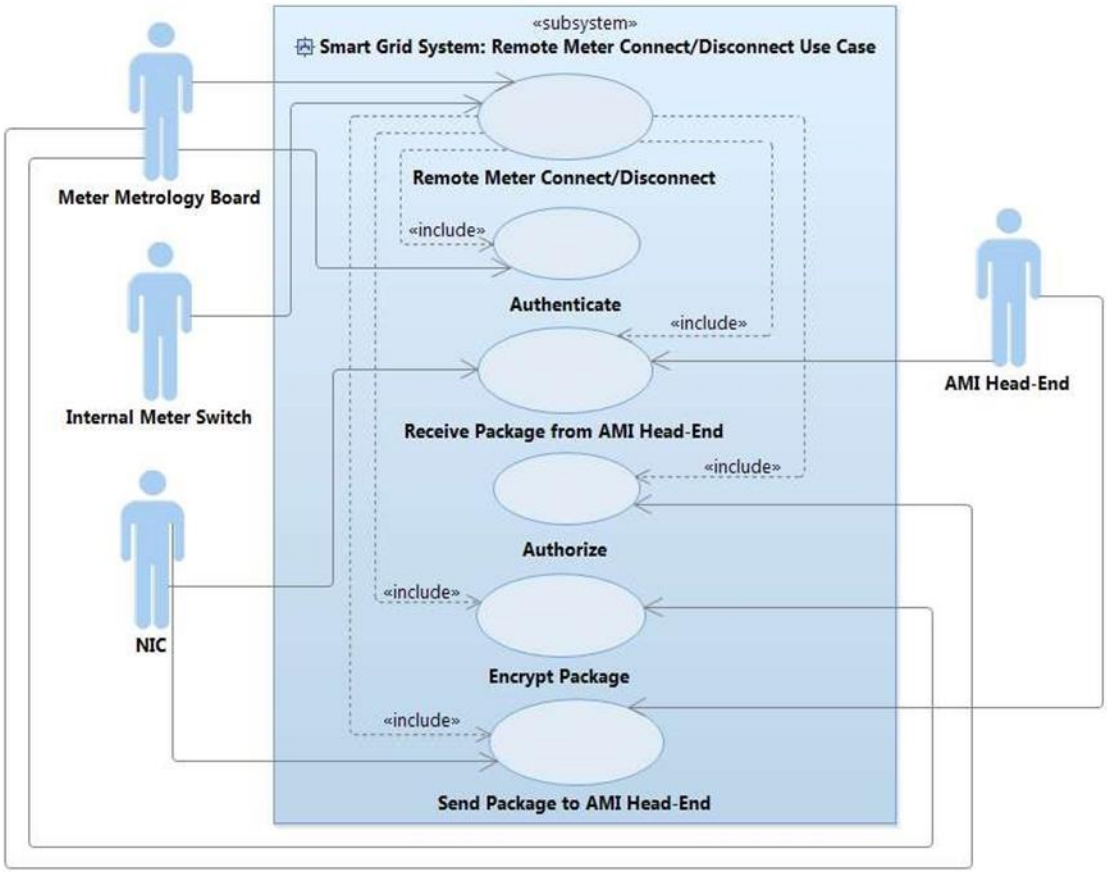


Fig 3.14 remote meter disconnect

On-Demand Meter Reading Use Case Diagram

Summary

On-demand meter reading is similar to periodic meter reading. The difference is that in on-demand meter reading, the process of meter reading is based on the demand. There is a demand on a specific date and time. The main use case in this use case diagram is “On-Demand Meter Reading”. This use case includes “Authenticate”, “Receive Package from AMI Head-End”,

"Authorize", "Encrypt Package", and "Send Package to AMI Head-End" use cases. NIC is the primary actor. Meter metrology board and AMI head-end are the secondary actors.

Description of use cases

In "On-Demand Meter Reading" use case, NIC receives the on-demand meter read request message from AMI head-end. Then meter metrology board retrieves meter read data in formatted table. NIC encrypts meter read data and it sends the on-demand meter read data to AMI head-end.

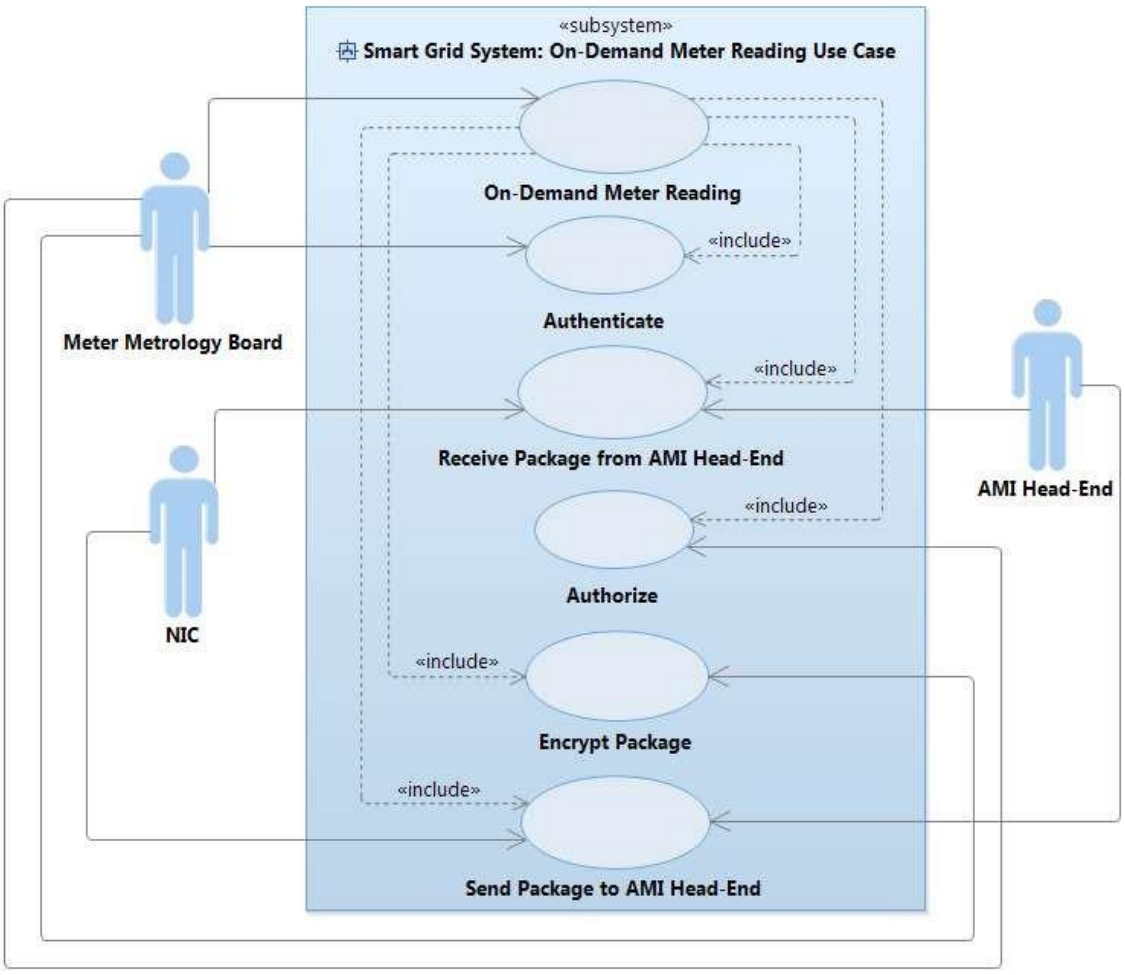


Fig 3.15 On-Demand Meter Reading Use Case Diagram

CHAPTER 4 CASE STUDY AND EXAMPLE

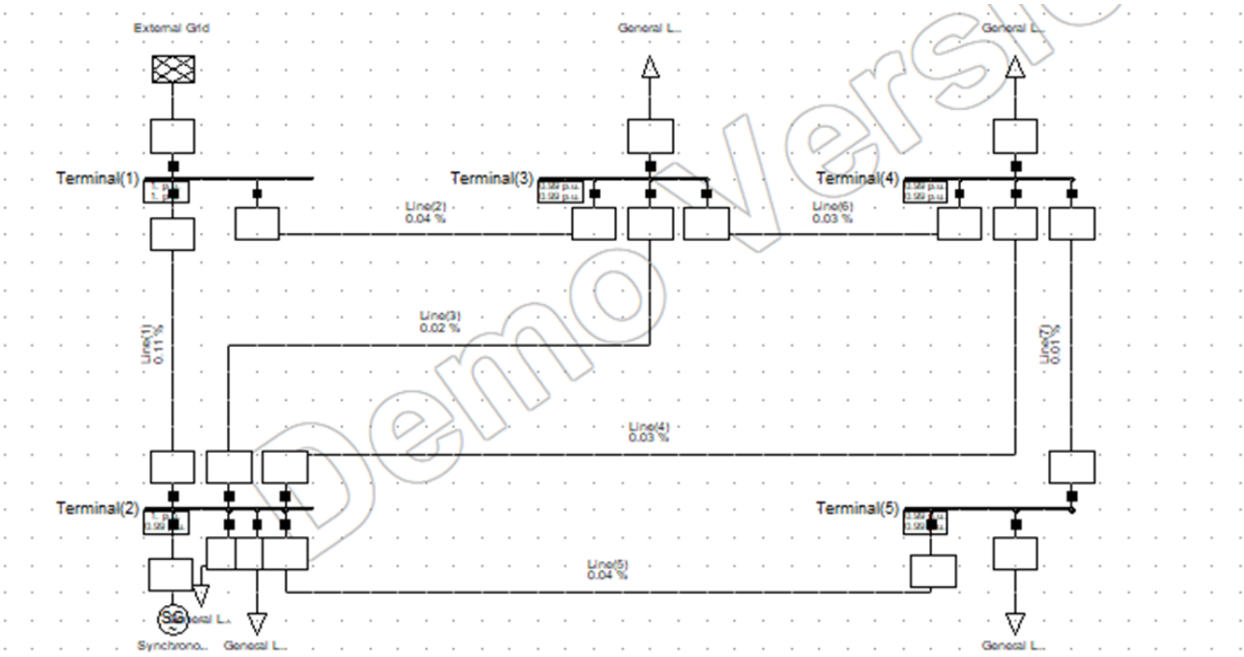


Fig 4.1 5 bus distribution system

Name	Active power MW	Reactive power MVar
load 1	0.045	0.015
load 2	0.04	0.05
Load 3	0.06	0.01
Load 4	0.01	0.01

1.In this case study I took a five bus distribution system we see how attacker has the ability to change the smart meter readings and change the internal home automation system.

2.He is able to control load at the user end by switching the load according to his desire he is tries to cause havoc to system.

3.One effect we are trying to we are taking to consideration is how generation has to change with change in load.

4. If the load is changing gradually the smart grid has to adopt to it and change the its generation in similar fashion.

5. Attacker has the control of loads and the system operator trying to increase or decrease. As the per the load so the cause could be the stability of system can be loss or in extreme cause the lines to overload and the machines or external grid can have wear and tear into it and its performance can be deteriorate over time

RESULTS

EXTERNAL GRID PLOT

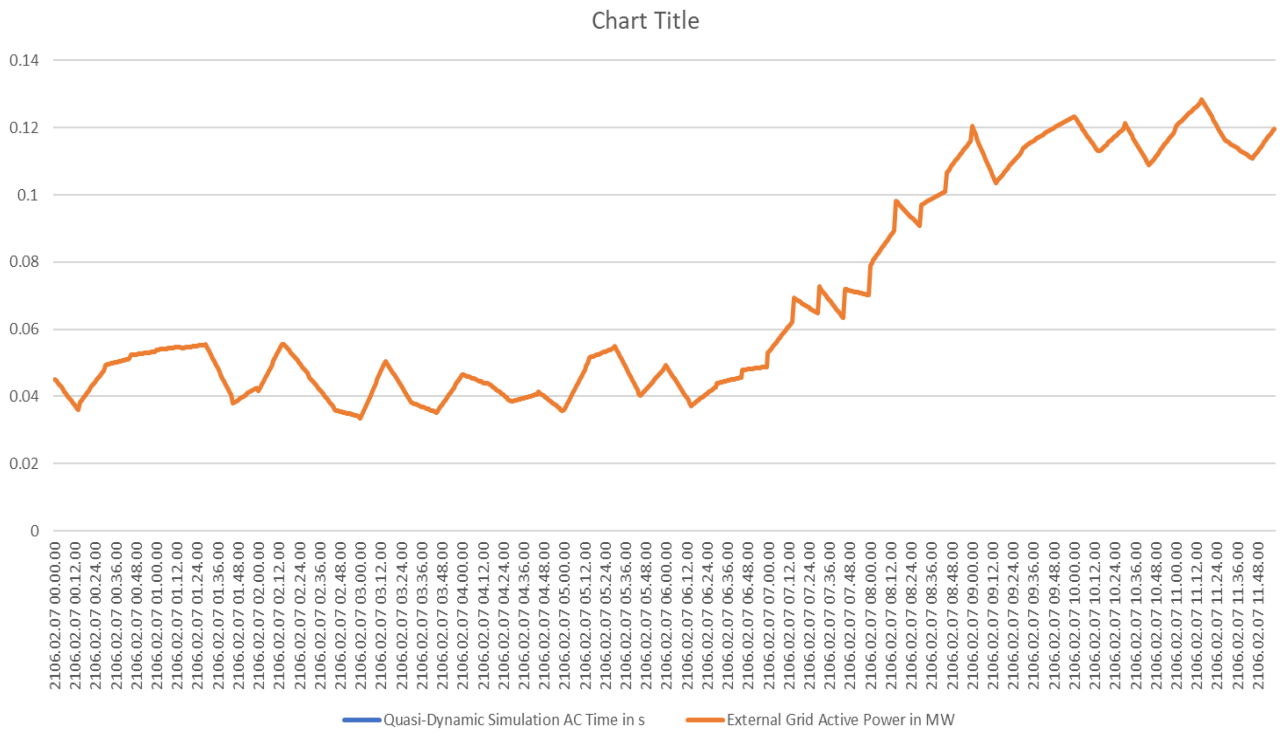


Fig 4.2 external grid plot

In external grid this is how the generation active power is varying with respect to time.

LOAD AT TERMINAL 2

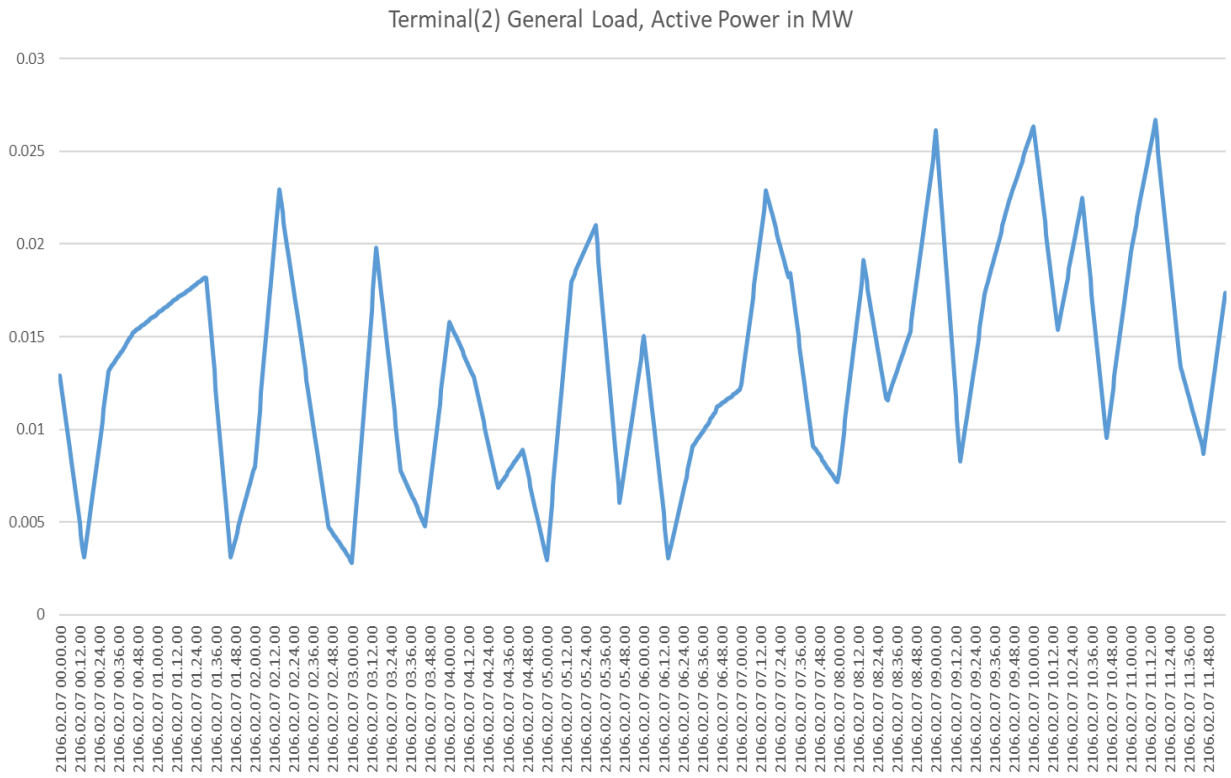


Fig 4.3 load at terminal 2 plot

This is how the attacker is trying to manipulate the load and because the load is manipulating there is stress on the generation to increase and decrease rapidly this might cause the stability issue and external grid deteriorate its performance.

DAILY LOAD CURVE CHARACTERISTICS

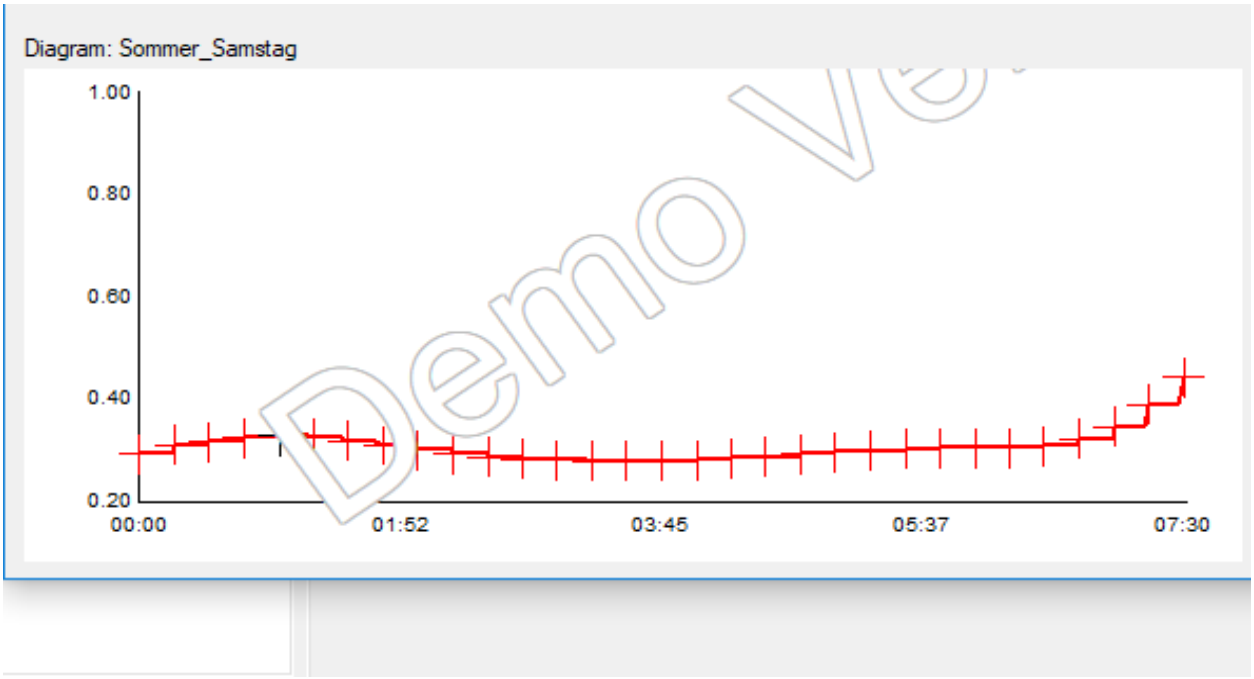


Fig 4.4 Daily load curve characteristics

ATTACK CHARACTERISTICS

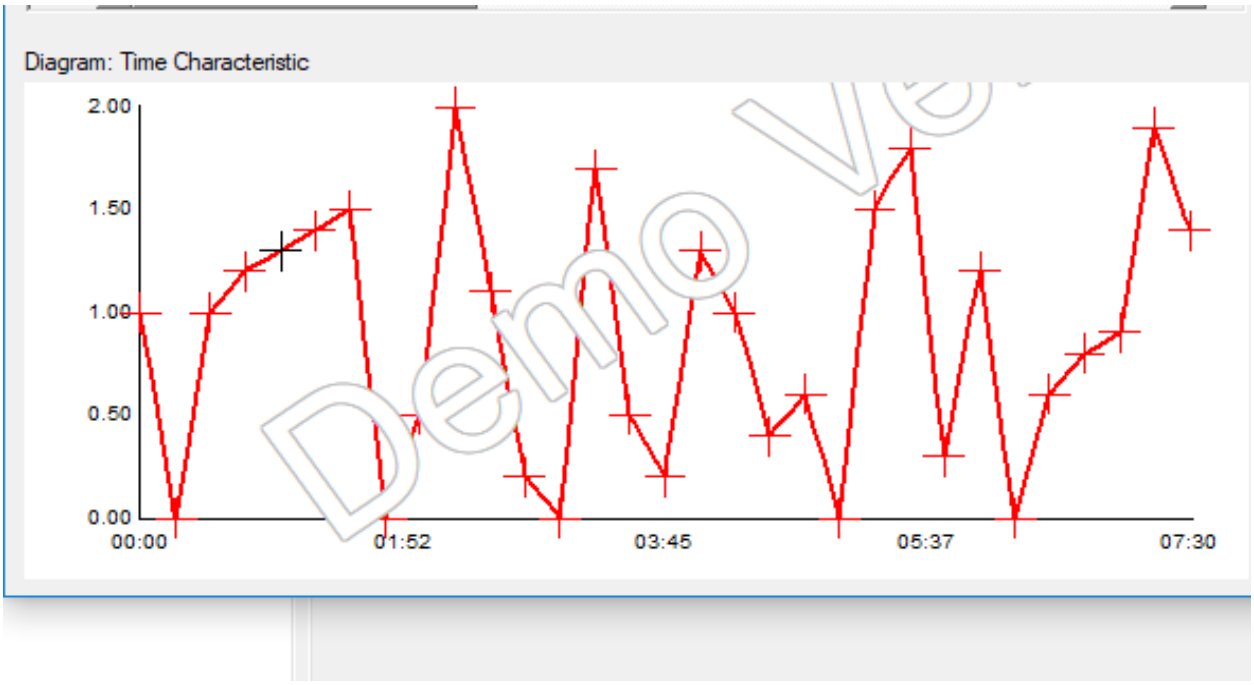


Fig 4.5 attack characteristics

CHAPTER 5 Conclusion and future work

In this thesis, we worked on the specific application of CPSs called smart grid. Smart grids generate electricity power and transmit this power to different categories of customers such as industries, factories, houses, etc. We specifically focused on main parts of smart grid systems and we showed how the attacker can cause harm to system by changing load which will result in losing the stability of the system.

In future work, we want to collect more information in the case of security design and to find the best and optimal solutions regarding to each security requirement with taking into account different factors such as the cost of security solutions, the performance of each security implementation solution, etc.

REFERENCES

1, Hahn, A. and M. Govindarasu, Cyber attack exposure evaluation framework for the smart grid. Smart Grid, IEEE Transactions on, 2011. 2(4): p. 835-843.

2. Güngör, V.C., et al., Smart grid technologies: communication technologies and standards. Industrial informatics, IEEE transactions on, 2011.

3. Berthier, R. and W.H. Sanders. Specification-based intrusion detection for advanced metering infrastructures. in Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on. 2011. IEEE

4.Smart Grids: A Cyber–Physical Systems Perspective By Xinghuo Yu, Fellow IEEE, and Yusheng Xue, Member IEEE

5. Hartmann, T., et al. Generating realistic smart grid communication topologies based on realdata. in Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on. 2014. IEEE

6. Wang, W. and Z. Lu, Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 2013.

7. Zafar, N., et al., System security requirements analysis: A smart grid case study. Systems Engineering,

8. Lu, R., et al., Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Transactions on Parallel and Distributed Systems,

9. Efthymiou, C. and G. Kalogridis. Smart Grid Privacy via Anonymization of Smart Metering Data. in 2010 First IEEE International Conference on Smart Grid Communications.

10. Berardi, D., D. Calvanese, and G. De Giacomo, Reasoning on UML class diagrams. Artificial Intelligence.