Security Governance
Master of Science in Cyber Security

AA 2023/2024

CYBER-RISK MANAGEMENT: A CASE STUDY

Study Case: Advanced Metering Infrastructure (AMI) in a Smart Grid

A *smart grid* is an electricity distribution network that can monitor the flow of electricity within itself and automatically adjust to changing conditions

An important component of the Smart Grid is the AMI

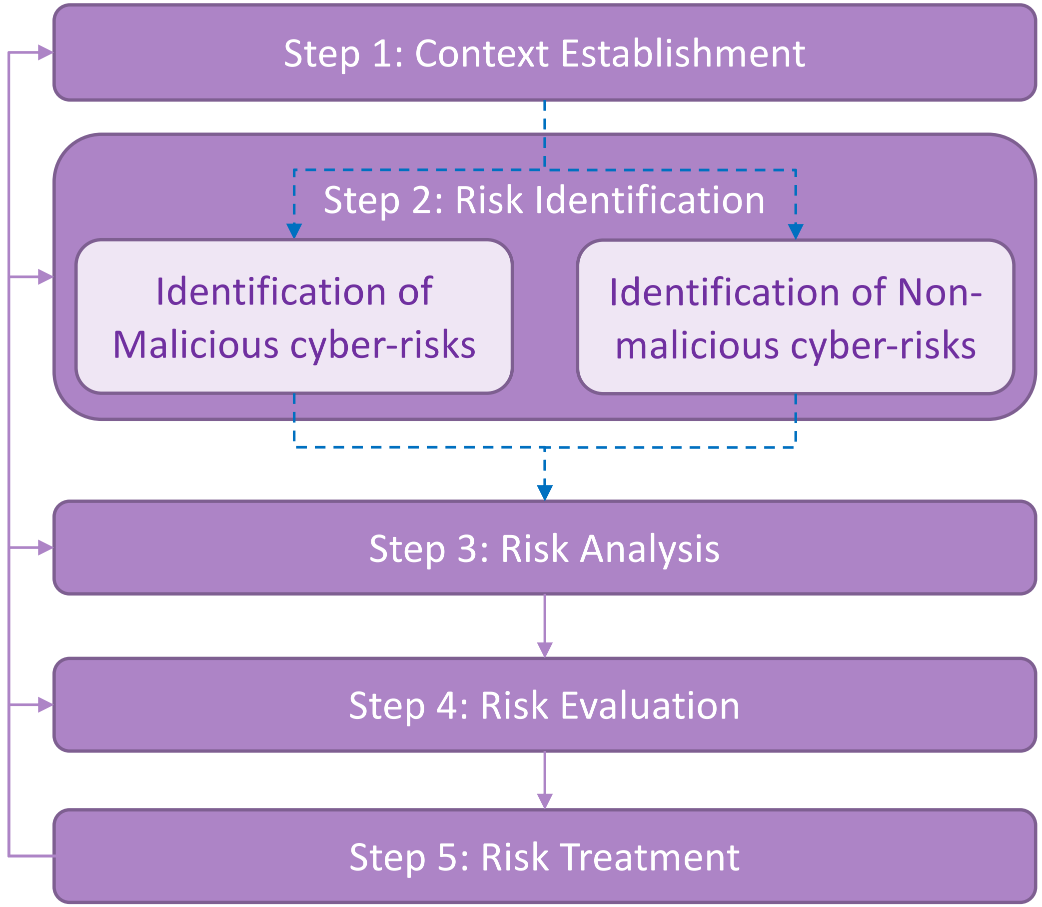
- AMI consists of power meters that use two-way communication to collect information related to electric power usage from electricity customers and also to provide information to these customers

OUR AIM: assess risks for such an infrastructure, which includes components for switching on/off power to an electricity customer or limiting the amount of power provided (choking)

↓

PARTY: distribution system operator

Recap: Cyber-Risk Assessment



Context Establishment

STEP 1

Recap: Context Establishment steps

1. Context Identification and Description
   - External Context
   - Internal Context
2. Definition of the Assessment Goals and Objectives
3. Target , Scope and Focus of Assessment Definition
4. Assumptions
5. Assets Identification
6. Definition of the Likelihood Scale
7. Definition of the Consequence Scale
8. Definition of the Risk Evaluation Criteria

External Context

External Context: description of societal, legal, regulatory, and financial environment and of the relationships with external stakeholders

A smart grid is a cyber-physical system that is part of a critical infrastructure.

The distribution system operator (our party) is subject to a number of national laws and regulations governing its operations (E.g., NIS in Europe)

- it is important to identify and document these laws and regulations
- Failure to comply may have significant legal and financial consequences, in the worst case putting the operator out of business.

Power outages or incidents (i.e., charging the wrong amount or disclosing electricity customer data) can damage the reputation and public trust in the operator.

Internal Context

Internal context: description of relevant goals, objectives, policies, and capabilities that may determine how risk should be assessed

Party's Mission: distributing electrical power to electricity customers.

The overall goals of the operator are:

1. to provide power in a reliable manner so that the electricity customers do not experience unintended power failures
2. to exchange correct and timely information with customers at all times so that they can be charged the right amount
3. to protect the privacy of its customers.

Most of the employees of the distribution system operator have strong technical competence and a few of the staff have received special training in risk assessment.

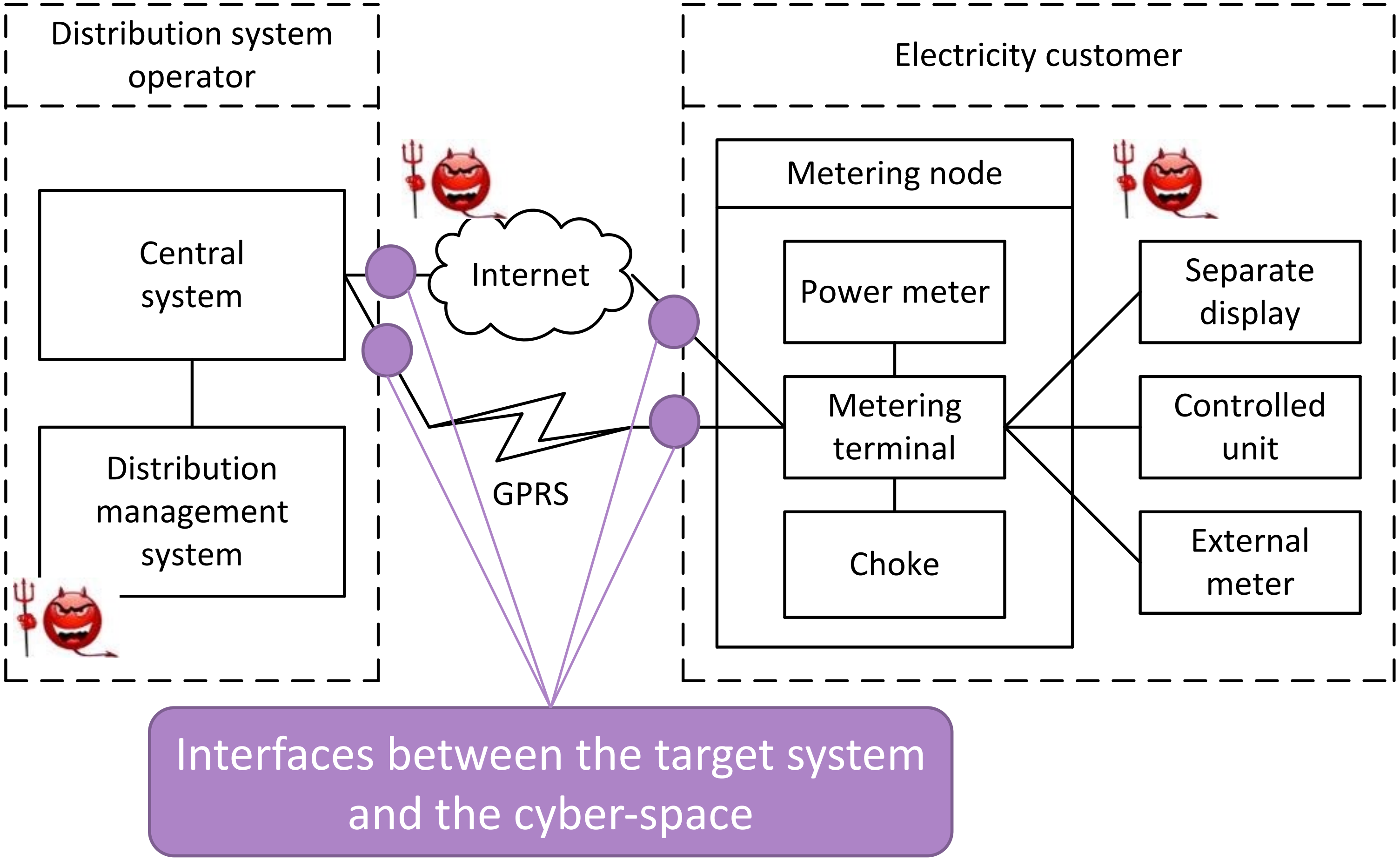
Goals and Objectives of the Assessment

1. Assess Risks wrt the business continuity
   - The assessment should help to reduce the risk of incidents that may impact the business of the distribution system operator, by identifying appropriate treatments for the important risks.

2. Law and regulation compliance

3. Improve Situation Awareness
   - the risk assessment should be documented in a way that can be understood by a wide range of internal and external stakeholders (including those who are not themselves experts on cybersecurity or smart grids)
   - Technical details should therefore be avoided as far as possible

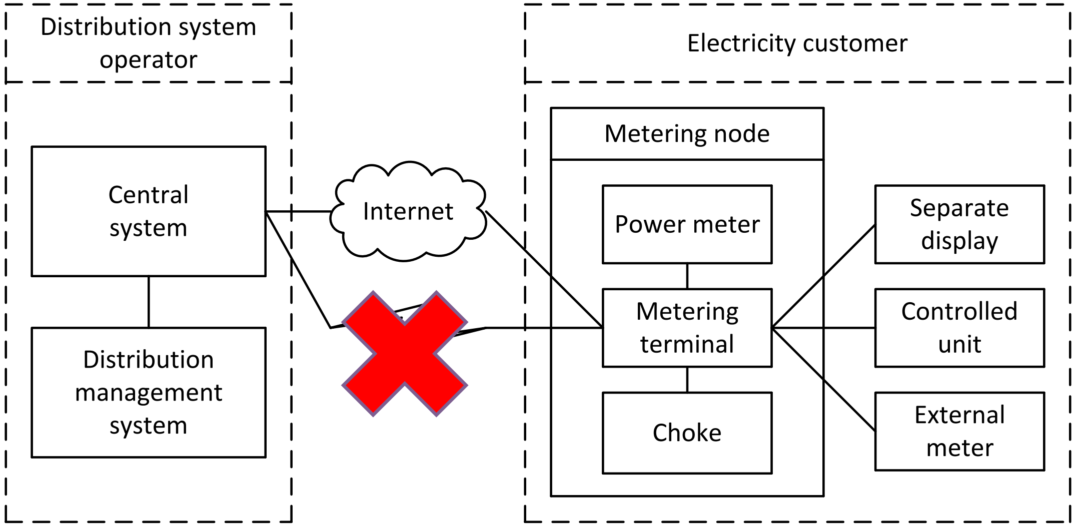
Target of the Assessment



Scope of the Assessment

We limit the scope of the assessment to risks due to attacks on or via the target of assessment

- Other attacks (e.g., attacks via back- end systems) are outside the scope of the assessment.
- Communication between Central system and Metering node via GPRS is supposed to be subject to a separate assessment and is therefore also outside our scope.



Focus of the Assessment

1. Exchange of meter data and control data via the Internet and the ways in which this may affect the provisioning of power, as the distribution system operator is particularly concerned about this aspect.
2. Although within the scope, the main focus will not be on attacks via physical access to components.
3. Risks caused by malicious as well as non-malicious threat sources should be considered.
4. Regarding functionality, the focus of the assessment is on basic AMI functions, which include
   - registering electricity customer meter data
   - transfer of data between **Electricity customer** and **Distribution system operator**
   - switching on/off or choking of power provided to the electricity customer.

Assumptions

1. threat sources may be both internal and external
2. malicious and non-malicious threats may be both internal and external
3. the target of assessment may be targeted not only by individuals with a purely financial or personal motive, but also by actors who wish to disrupt society.
4. all meter data and control data sent between the central system and metering nodes are encrypted.

Assets

NOTE: The distribution system operator is the sole party for the cyber-risk assessment, which means that all consequence assessments and risk evaluation criteria will be defined from that perspective

ASSET	DESCRIPTION
Integrity of meter data	The integrity of meter data should be protected all the way from **Power meter** to **Distribution system operator**
Availability of meter data	Meter data from **Metering node** should be available for **Distribution system operator** at all times
Provisioning of power to electricity customers	Power should only be switched off or choked as a result of legitimate control signals from **Central system**

Likelihood Scale

For this risk assessment we specify likelihood in terms of frequencies

Likelihood value	Description
Rare	Less than once per ten years
Unlikely	Less than once per two years
Possible	Less than twice per year
Likely	Two to five times per year
Certain	Five times or more per year

five-step scales of intervals for likelihood

- we need only determine which interval the likelihood of an incident lies within, rather than providing an exact value.
- It is a simple way of expressing the uncertainty

the granularity of the chosen scales depends on availability of data and the preferences of the decision makers

Consequence Scales

RECALL: Consequences are related to Assets

We need to define one consequence scale for each identified Asset

RECALL: Scales are defined from the perspective of the distribution system operator, which considers the overall business impact of potential incidents

Consequence Scales

Table 6.4 Consequence scale for integrity of meter data

Consequence value	Description
Insignificant	Errors in meter data for up to 100 electricity customers
Minor	Errors in meter data for 101-2,000 electricity customers
Moderate	Errors in meter data for 2,001-20,000 electricity customers
Major	Errors in meter data for 20,001-50,000 electricity customers
Critical	Errors in meter data for more than 50,000 electricity customers

Consequence Scales

Table 6.5 Consequence scale for availability of meter data

Consequence value	Description
Insignificant	Meter data for up to 1,000 electricity customers unavailable for 1-24 hours
Minor	Meter data for up to 1,000 electricity customers unavailable for more than 1 day or meter data for 1,001-10,000 electricity customers unavailable for 1-24 hours
Moderate	Meter data for 1,001-10,000 electricity customers unavailable for more than 1 day or meter data for more than 10,000 electricity customers unavailable for 1-24 hours
Major	Meter data for more than 10,000 electricity customers unavailable for 25 hours-7 days
Critical	Meter data for more than 10,000 electricity customers unavailable for more than 7 days

Consequence Scales

Table 6.6 Consequence scale for provisioning of power to electricity customers

Consequence value	Description
Insignificant	Power outage for up to 100 electricity customers for 1-24 hours
Minor	Power outage for up to 100 electricity customers for more than 24 hours or power outage for 101-1,000 electricity customers for 1-24 hours
Moderate	Power outage for 101-1,000 electricity customers for more than 24 hours or power outage for 1,001-10,000 electricity customers for 1-24 hours
Major	Power outage for 1,001-10,000 electricity customers for 25-72 hours or power outage for more than 10,000 electricity customers for 1-24 hours
Critical	Power outage for 1,001-10,000 electricity customers for more than 72 hours or power outage for more than 10,000 electricity customers for more than 24 hours

Risk Evaluation Criteria

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical					
	Major					
	Moderate					
	Minor					
	Insignificant					

Risk Identification

STEP 2

Risk Identification

The goal is to arrive at a collection of

- threat sources
- threats
- vulnerabilities
- incidents
- risks

that is as correct and complete as possible for our particular target of assessment and assets

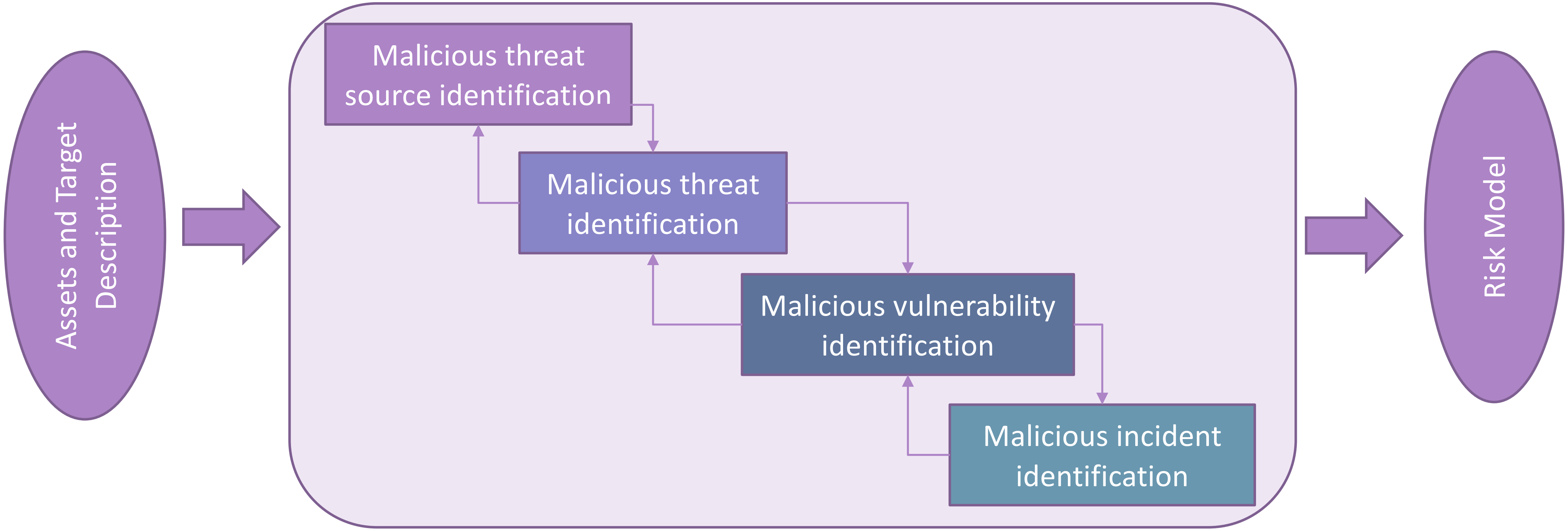
Risk Identification Techniques

In order to identify risks we should gather information about the environment

- Logs, intrusion detection systems (IDSs) and other monitoring tools, vulnerability scanners, results from penetration tests or other kinds of security tests, source code reviews…
- External Vulnerability and Threats Repositories
- extract information from people who know the target of assessment well from their particular viewpoints

When using historical data such as event logs, you should take great care not to fall into the trap of believing that tomorrow will be like yesterday

Identification of Malicious Cyber-risk



Threat Source Identification

Understand who may want to initiate attacks and why

The potential for causing harm will depend on

- the motive and intention of the threat sources
- their capabilities
- available resources

It is therefore important to document these characteristics in the threat source descriptions

Threat Source Identification

Table 7.2 Malicious threat sources

Threat source	Motive and intention	Capability and resources

Threat Source Identification

Hacktivist	Similarly to cyber-terrorists, hacktivists are motivated by a political, ideological, or religious agenda and use cyber-attacks to achieve their goals. Although the distinction between cyber-terrorists and hacktivists is fuzzy at best, we assume that hacktivists are less willing to go to extremes and that their aim is to harm selected groups, politicians, or other individuals, rather than society as a whole	Skill level and resources can vary a lot. Most hacktivists are assumed to operate alone or in small or poorly organized groups. However, if well organized they can potentially have access to significant computational resources as well as competence

Threat Identification

For each malicious threat source we identify the threats it may initiate

focus on how the threat sources may exploit the attack surface identified during the context establishment

Table 7.3 Malicious threats

Threat source	Attack point	**Threat**
Script kiddie	Internet connection to the central system	DDoS attack on the central system
Cyber-terrorist	Same as the row above	Same as the row above
Cyber-terrorist	Internet connection between the central system and the metering terminal	Tampering with all or most control data in transit from the central system to the choke component
Black hat hacker	Internet connection between the central system and the metering terminal	Tampering with data in transit from the metering terminal to the central system
Black hat hacker	Communication line between the metering terminal and the external meter	Malware to manipulate meter data is installed on the metering terminal through connection to the external meter
Malware	Internet connection to the metering terminal	Metering node infected by malware
Hacktivist	Internet connection between the metering terminal and the central system	Tampering with control data in transit from the central system to the choke components for selected electricity customers
Insider	Central system	Illegitimate control data sent to the choke components from the central system

Vulnerability identification

For each malicious threat we identify the existing vulnerabilities that the threat may exploit.

The identification may start from looking to Vulnerability lists such as

- NISTIR 7628 guidelines for smart grid cybersecurity
- ISO 27005 (it offers a list of vulnerabilities related to hardware, software, network, personnel, site, and organization)
- Online resources offered by OWASP (http://www.owasp.org)
- Common Weakness Enumeration (CWE) offered by MITRE

Vulnerabilities may also be identified by scanners or as output of testing activities

Vulnerability identification

Table 7.4 Vulnerabilities with respect to malicious threats

Threat	**Vulnerability**	Description
DDoS attack on the central system	Inadequate attack detection and response on central system	New forms of DDoS attacks are continuously being developed to defeat existing countermeasures. Due to the challenges of keeping the central system running 24/7, combined with the lack of a strong tradition for cybersecurity awareness in the power distribution domain (which has not traditionally operated in cyberspace), countermeasures to various forms of DDoS attacks on the central system are rarely updated and may therefore be out of date
Tampering with all or most control data in transit from the central system to the choke component	Weak encryption and integrity check	The encryption of messages between the central system and the metering node may be weak compared to the current standard. The same applies to the integrity checking of received messages. This applies in particular at the metering nodes, which have relatively little computing power and are rarely replaced
Tampering with data in transit from the metering terminal to the central system	Weak encryption and integrity check	The considerations here are the same as in the previous row

Vulnerability identification

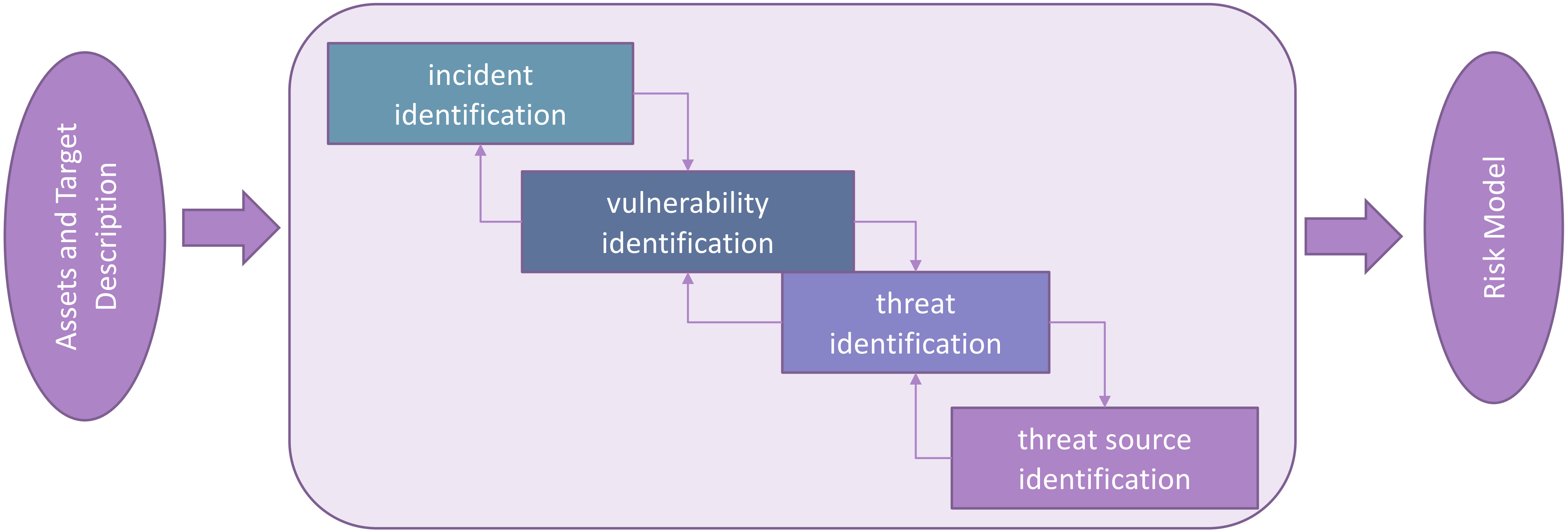
Tampering with control data in transit from the central system to the choke components for selected electricity customers	Weak encryption and integrity check	The considerations here are the same as in the previous row
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Unprotected local network, no sanitation of input data from the external meter	The local network at the electricity customer location cannot be assumed to be properly protected, as this depends on the individual customer. Moreover, data from the external meter to the metering terminal are not adequately sanitized before further processing, thereby leaving the metering terminal vulnerable to code injection attacks
Metering node infected by malware	Outdated antivirus protection on metering node	The metering node is connected to the Internet in order to communicate with the central system and is therefore susceptible to malware. However, the virus protection on the metering node is rarely updated
Illegitimate control data sent to the choke components from the central system	Four-eyes principle not implemented, no logging of actions of individual central system operators	The operating procedures and technical implementation of the central system do not enforce approval of control data by a second authorized person. An operator is therefore able to send control data that are not legitimate. Moreover, there is no logging of the actions of individual operators

Incident Identification

Table 7.5 Incidents caused by malicious threats

Threat	**Incident**	Asset
DDoS attack on the central system	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data
Tampering with all or most control data in transit from the central system to the choke component	False control data received by all or most choke components	Provisioning of power to electricity customers
Tampering with data in transit from the metering terminal to the central system	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Same as the row above	Same as the row above
Metering node infected by malware	Malware compromises meter data	Integrity of meter data
Metering node infected by malware	Malware disrupts transmission of meter data	Availability of meter data
Metering node infected by malware	Malware disrupts the choke functionality	Provisioning of power to electricity customers
Tampering with control data in transit from the central system to the choke components for selected electricity customers	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers
Illegitimate control data sent to the choke components from the central system	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers

Identification of Non-malicious Cyber-risk



Incident Identification

Table 7.7 Incidents caused by non-malicious threats

Asset	**Incident**	Description
Provisioning of power to electricity customers; Availability of meter data	Communication between the central system and the metering terminal is lost	Provisioning of power to the electricity customer depends on control data being sent from the central system to the metering terminal. Availability of meter data depends on such data being sent in the opposite direction
Integrity of meter data	Software bug on the metering terminal compromises meter data	Metering terminals run software to register meter data and transmit these to the central system. Software bugs on metering terminals may therefore compromise meter data
Availability of meter data	Software bug on the metering terminal disrupts transmission of meter data	Similarly to the above case, software bugs on metering terminals may disrupt transmission of meter data to the central system
Provisioning of power to electricity customers	Software bug on the metering terminal disrupts the choke functionality	Control signals to the choke component from the central system go via the metering terminal. Software bugs on metering terminals may therefore disrupt the choke functionality by not forwarding correct control signals
Provisioning of power to electricity customers	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Maintenance mistakes such as misconfiguration of communication parameters may prevent or disrupt transmission of control data
Availability of meter data	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Maintenance mistakes such as misconfiguration of communication parameters may prevent metering node data from being received
Provisioning of power to electricity customers; Availability of meter data	The metering terminal goes down due to damage from lightning	Lightning may result in physical damage to the metering terminal which prevents it from functioning

Risk Analysis

STEP 3

Recap: Risk Analysis

The risk analysis is the activity aiming to estimate and determine the level of the identified risks

Observation 1: the risk level is derived from the combination of the likelihood and consequence

Risk Estimation

Likelihoods Estimation + **Consequences Estimation**

Risk Analysis

Goal: assess the likelihood of the identified incidents and their consequence for each of the affected assets

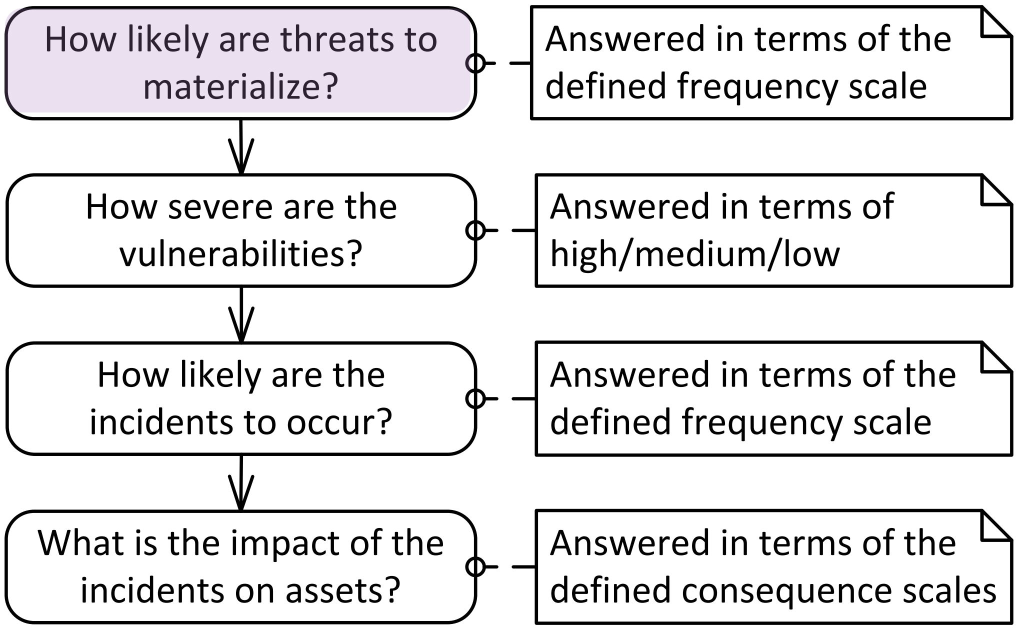
Information sources: same as those used for risk identification.

The main difference is that now we also need to consider

- the severity of vulnerabilities
- likelihood of threats and incidents
- consequence of incidents

Risk Analysis process

According with the scales identified in the Context Establishment phase, we proceed by answering to the following questions:



Malicious Threat Analysis

Main sources of information for the likelihood estimation:

- event logs provided by the distribution system operator
- expert judgments of the participants

We choose to follow an approach inspired by the OWASP risk-rating method[1]

- The factors are rated on a scale from 0 to 9.

1 - https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Malicious Threat Analysis

Factors	Description
Skill Level	How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
Motive	How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
Opportunity	What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
Size	How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Malicious Threat Analysis

Let’s now analyse each row of the Table relating Threats and Threat Sources

Table 7.3 Malicious threats

Threat source	Attack point	**Threat**
Script kiddie	Internet connection to the central system	DDoS attack on the central system
Cyber-terrorist	Same as the row above	Same as the row above
Cyber-terrorist	Internet connection between the central system and the metering terminal	Tampering with all or most control data in transit from the central system to the choke component
Black hat hacker	Internet connection between the central system and the metering terminal	Tampering with data in transit from the metering terminal to the central system
Black hat hacker	Communication line between the metering terminal and the external meter	Malware to manipulate meter data is installed on the metering terminal through connection to the external meter
Malware	Internet connection to the metering terminal	Metering node infected by malware
Hacktivist	Internet connection between the metering terminal and the central system	Tampering with control data in transit from the central system to the choke components for selected electricity customers
Insider	Central system	Illegitimate control data sent to the choke components from the central system

Malicious Threat Analysis

Threat: DDoS attack on the central system

Threat Source: script kiddie

Script kiddie	Achieve status among a group or prove his/her ability to cause harm. Will seldom be very persistent if faced with difficulties and initial failure	Relatively unskilled, unable to perform complicated attacks. Typically uses tools developed by others to initiate attacks. Very limited access to computational or monetary resources

Factors	Score [1, 9]	Rationale
Skill Level	3	She/he is relatively unskilled and unable to perform complicated attacks
Motive	1	Motive generally weak
Opportunity	7	She/he has enough resources and opportunities to conduct the attack (low cost)
Size (i.e., it is a measure of how large this group of threat sources is)	7	script kiddies can reside anywhere in the world
AVG	4,5	

Malicious Threat Analysis

Let’s now analyse each row of the Table relating Threats and Threat Sources

Table 7.3 Malicious threats

Threat source	Attack point	**Threat**
Script kiddie	Internet connection to the central system	DDoS attack on the central system
Cyber-terrorist	Same as the row above	Same as the row above
Cyber-terrorist	Internet connection between the central system and the metering terminal	Tampering with all or most control data in transit from the central system to the choke component
Black hat hacker	Internet connection between the central system and the metering terminal	Tampering with data in transit from the metering terminal to the central system
Black hat hacker	Communication line between the metering terminal and the external meter	Malware to manipulate meter data is installed on the metering terminal through connection to the external meter
Malware	Internet connection to the metering terminal	Metering node infected by malware
Hacktivist	Internet connection between the metering terminal and the central system	Tampering with control data in transit from the central system to the choke components for selected electricity customers
Insider	Central system	Illegitimate control data sent to the choke components from the central system

Malicious Threat Analysis

Threat: DDoS attack on the central system

Threat Source: cyber-terrorist

Cyber-terrorist	Cause disruption in a society through cyber-attacks, preferably against critical infrastructure. Strong political, ideological, or religious motives and willingness to go to extremes	May command significant resources and skill, in some cases even being supported by nation states. Able to perform long-term planning, preparation, and carrying out of attacks

Factors	Score [1, 9]	Rationale
Skill Level	7	May command significant resources and skill, in some cases even being supported by nation states. Able to perform long-term planning, preparation, and carrying out of attacks
Motive	8	
Opportunity	7	
Size (i.e., it is a measure of how large this group of threat sources is)	3	Cyber-terrorist are far less than script kiddie
AVG	6,25	

Malicious Threat Analysis

Based on these results (4,5 and 6,25), considering the worse case, and using our own likelihood scale, we estimate the likelihood of this threat to be *Likely*

Likelihood value	Description	
Rare	Less than once per ten years	0 - 1,8
Unlikely	Less than once per two years	1,8 – 3,6
Possible	Less than twice per year	3,6 – 5,4
Likely	Two to five times per year	5,4 – 7,2
Certain	Five times or more per year	7,2 - 9

check that the estimate is supported by the available event logs and confirmed by the participants from the distribution system operator

Malicious Threat Analysis

Iterating over all the Threats identified we get the following estimation

Threat	Likelihood
DDoS attack on the central system	Likely
Tampering with all or most control data in transit from the central system to the choke component	Possible
Tampering with data in transit from the metering terminal to the central system	Possible
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Possible
Metering node infected by malware	Rare
Tampering with control data in transit from the central system to the choke components for selected electricity customers	Unlikely
Illegitimate control data sent to the choke components from the central system	Unlikely

Non-Malicious Threat Analysis

For each identified threat, start by considering the threat source

Table 7.10 Non-malicious threat sources

Threat	**Threat source**	Description
Internet connection to the metering terminal goes down	Internet connection to the metering terminal	Problems with the connection may initiate threats to the communication between the metering terminal and central system
Buggy software distributed on metering terminals	Software bug	Any kind of software error or malfunction that arises due to mistakes rather than malicious intent
Mistakes during update/maintenance of the central system	Maintenance personnel	Persons responsible for maintaining the computer systems and infrastructure for the distribution system operator. They do not seek to cause harm, but may still do so by mistake, neglect, or lack of proper training. Notice that a maintenance person with malicious intent is considered to be an insider with respect to this risk assessment
Electricity customer home/building is struck by lightning	Lightning	Strokes of lightning which may have potential for causing damage to computerized systems and network infrastructure

Non-Malicious Threat Analysis

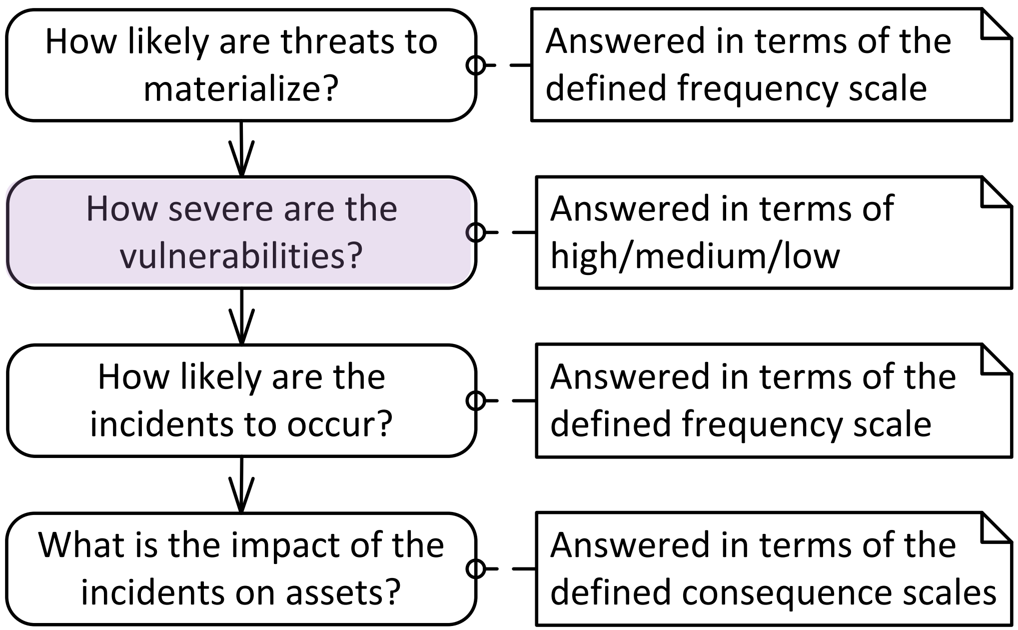
To estimate the Likelihood, it is possible to consider information such as event logs, expert judgments, interviews or questionnaires, and available statistics about the typical likelihood of similar threats in enterprises and other organizations.

Table 8.2 Non-malicious threat analysis

Threat	**Likelihood**	Estimate basis/comments
Internet connection to the metering terminal goes down	Certain	This includes cases where individual electricity customer's homes lose Internet connection, which according to general statistics happens very often
Buggy software distributed on metering terminals	Possible	This estimate is based on patching logs for various software products developed by the provider of metering terminal software during the last four years
Mistakes during update/maintenance of the central system	Certain	This estimate is based on event logs and statements from the head of the management team
Electricity customer home/building is struck by lightning	Certain	This estimate is based on statistics for the geographical area where the electricity customers are located

Risk Analysis process

According with the scales identified in the Context Establishment phase, we proceed by answering to the following questions:



Vulnerability Analysis

The next step consists of analysing vulnerabilities.

For this we choose to use a simple scale consisting of the steps High, Medium, and Low

Severity	Score
0-3	Low
3-6	Medium
6-9	High

Malicious Threat Vulnerabilities

To provide Vulnerability severity estimation we can use as information sources:

- expert judgments, statistics, and open repositories
- vulnerability scans, security testing, penetration testing, and code review

Inspired by the OWASP risk-rating method we rate vulnerabilities as follow

Factors	Description
ease of discovery	How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
ease of exploit	How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
awareness	How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
intrusion detection	How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

Malicious Threat Vulnerabilities

As a result of the analysis done in step 2 Risk Identification, we identified 5 different vulnerabilities associated to the malicious threats

1. Inadequate attack detection and response on central system
2. Weak encryption and integrity check
3. Unprotected local network, no sanitation of input data from the external meter
4. Outdated antivirus protection on metering node
5. Four-eyes principle not implemented, no logging of actions of individual central system operators

Let’s analyse them one by one

Malicious Threat Vulnerabilities

Vulnerability*:* Inadequate attack detection and response on central system

Factors	Score [1, 9]	Rationale
ease of discovery	7	Checking whether systems are vulnerable to DDoS attacks is often straightforward
ease of exploit	5	After conducting tests, we verified that this vulnerability can be exploited
awareness	6	knowledge of the existence of such vulnerabilities is widespread
intrusion detection	7	After Tests we verified that intrusions are usually not detected when they happen
AVG	6,25	

Malicious Threat Vulnerabilities

Iterating over all the Vulnerabilities identified we get the following estimation

Vulnerability	Severity
Inadequate attack detection and response on central system	High
Weak encryption and integrity check	Medium
Unprotected local network, no sanitation of input data from the external meter	Medium
Outdated antivirus protection on metering node	High
Four-eyes principle not implemented, no logging of actions of individual central system operators	High

Non-malicious Threat Vulnerabilities

Observation: For the non-malicious threats there is no intent to discover and exploit vulnerabilities

We try to understand the extent to which there is a lack of barriers that could prevent threats from leading to incidents

Non-malicious Threat Vulnerabilities

As a result of the analysis done in step 2 Risk Identification, we identified 4 different vulnerabilities associated to non-malicious threats

1. Single communication channel between central system and metering terminal
2. Poor Testing
3. Poor training and heavy workload
4. Inadequate overvoltage protection

In this case the assessment is done analysing the environment and making consideration over the processes in place

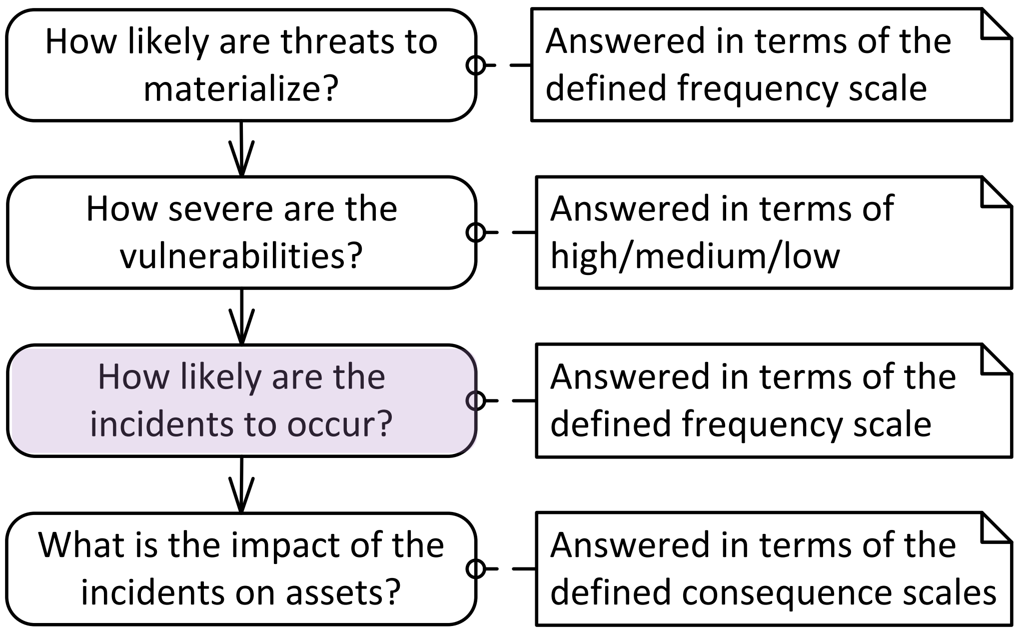
Non-malicious Threat Vulnerabilities

Table 8.4 Vulnerability analysis with respect to non-malicious threats

Vulnerability	**Severity**	Explanation
Single communication channel between central system and metering terminal	High	The Internet connection is the only communication channel to the central system for many electricity customers
Poor testing	Medium	Inspection of maintenance logs revealed a number of instances where bugs have been discovered in the metering terminal software. Previous experience indicates that the testing routines of the external software provider are unsatisfactory, and the central system operator does not test software updates for metering terminals before deployment
Poor training and heavy workload	Medium	Interviews indicate that security awareness is not high. Key persons have too much to do. Routines for reviewing and testing updates to the central system before deployment are strong
Inadequate overvoltage protection	High	The computing hardware of metering terminals is not robust with respect to transient overvoltage

Risk Analysis process

According with the scales identified in the Context Establishment phase, we proceed by answering to the following questions:



Likelihood of Incidents

In order to estimate the likelihood of incidents, we consider the analysis of threats that lead to the incidents and the vulnerabilities that the threats exploit

Table 7.9 Non-malicious threats

Incident	**Threat**	Entry point
Communication between the central system and the metering terminal is lost	Internet connection to the metering terminal goes down	Internet connection to the metering terminal
Software bug on the metering terminal compromises meter data	Buggy software distributed on metering terminals	Metering terminal
Software bug on the metering terminal disrupts transmission of meter data	Same as the row above	Metering terminal
Software bug on the metering terminal disrupts the choke functionality	Same as the row above	Metering terminal
Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Mistakes during update/maintenance of the central system	Central system
Mistakes during maintenance of the central system prevent reception of data from metering nodes	Same as the row above	Central system
The metering terminal goes down due to damage from lightning	Electricity customer home/building is struck by lightning	Metering terminal

Likelihood of Incidents caused by malicious threats

At the end of the Analysis done in step 2 Risk Identification we identified these incidents

Table 7.5 Incidents caused by malicious threats

Threat	**Incident**	Asset
DDoS attack on the central system	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data
Tampering with all or most control data in transit from the central system to the choke component	False control data received by all or most choke components	Provisioning of power to electricity customers
Tampering with data in transit from the metering terminal to the central system	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Same as the row above	Same as the row above
Metering node infected by malware	Malware compromises meter data	Integrity of meter data
Metering node infected by malware	Malware disrupts transmission of meter data	Availability of meter data
Metering node infected by malware	Malware disrupts the choke functionality	Provisioning of power to electricity customers
Tampering with control data in transit from the central system to the choke components for selected electricity customers	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers
Illegitimate control data sent to the choke components from the central system	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers

Likelihood of Incidents caused by malicious threats

Incident	Data from metering nodes cannot be received by the central system due to DDoS attack	
Threat	DDoS attack on the central system	Likelihood: Likely
Vulnerability	Inadequate attack detection and response on central system	Severity: High

Considerations

- Event logs show only two such incidents for the last three years (which corresponds to Possible)
- However, there is an increasing trend of this type of incidents
- Although the number of DDoS attacks that succeed will likely be lower than the number of attempts, we still estimate that the frequency for the incident also lies within the interval of Likely on our scale.

Likelihood of Incidents caused by non-malicious threats

At the end of the Analysis done in step 2 Risk Identification we identified these incidents

Table 7.9 Non-malicious threats

Incident	**Threat**	Entry point
Communication between the central system and the metering terminal is lost	Internet connection to the metering terminal goes down	Internet connection to the metering terminal
Software bug on the metering terminal compromises meter data	Buggy software distributed on metering terminals	Metering terminal
Software bug on the metering terminal disrupts transmission of meter data	Same as the row above	Metering terminal
Software bug on the metering terminal disrupts the choke functionality	Same as the row above	Metering terminal
Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Mistakes during update/maintenance of the central system	Central system
Mistakes during maintenance of the central system prevent reception of data from metering nodes	Same as the row above	Central system
The metering terminal goes down due to damage from lightning	Electricity customer home/building is struck by lightning	Metering terminal

Likelihood of Incidents caused by non-malicious threats

Incident	Mistakes during maintenance of the central system disrupt control signals to the choke component	
Threat	Mistakes during update/maintenance of the central system	Likelihood: Certain
Vulnerability	Poor training and heavy workload	Severity: Medium

Incident	Mistakes during maintenance of the central system prevent reception of data from metering nodes	
Threat	Mistakes during update/maintenance of the central system	Likelihood: Certain
Vulnerability	Poor training and heavy workload	Severity: Medium

Likelihood of Incidents caused by malicious threats

CONSIDERATIONS

- At first glance the two incidents seems to occur with the same frequency
- However, we found before that there are routines in place for reviewing and testing the system before changes are launched
- Considering that provisioning of power to the electricity customer is more critical than the continuous reading of meter data, the routines are stronger with respect to updates and changes that may affect control data
- This observation, combined with the data logs, leads us to the likelihood <u>Unlikely</u> regarding control data to the choke component, and the likelihood <u>Possible</u> regarding the reception of meter data

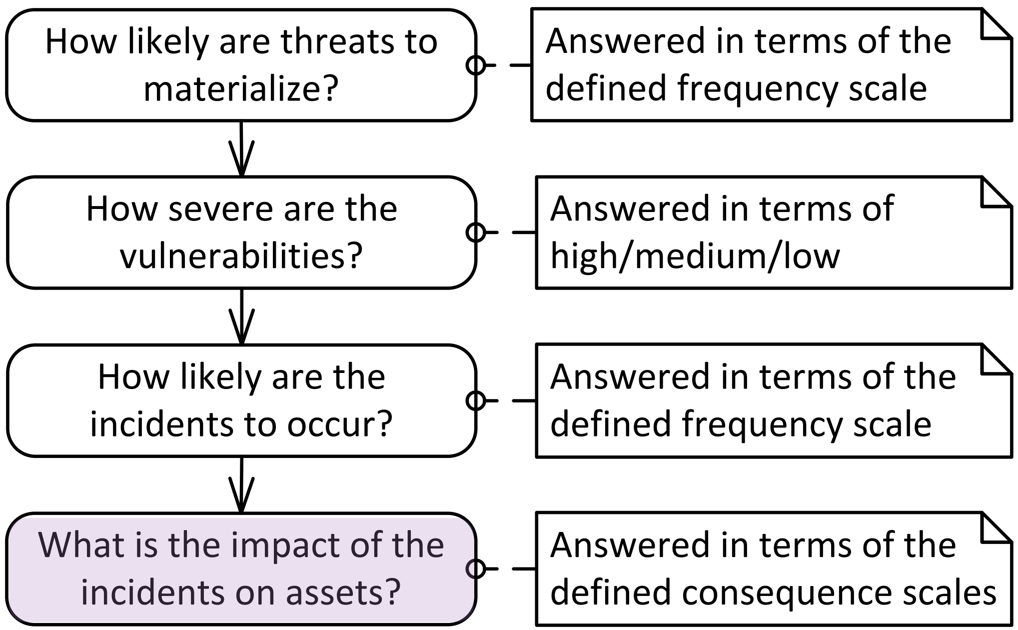
Likelihood of Incidents caused by non-malicious threats

Incident	Mistakes during maintenance of the central system disrupt control signals to the choke component	Likelihood: Unlikely
Threat	Mistakes during update/maintenance of the central system	Likelihood: Certain
Vulnerability	Poor training and heavy workload	Severity: Medium

Incident	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Likelihood: Possible
Threat	Mistakes during update/maintenance of the central system	Likelihood: Certain
Vulnerability	Poor training and heavy workload	Severity: Medium

Risk Analysis process

According with the scales identified in the Context Establishment phase, we proceed by answering to the following questions:



Consequences of Incidents

Recall: The consequence of an incident must be judged for each asset it harms.

At the end of the Analysis done in step 2 Risk Identification we identified these incidents harming the 3 identified assets

Threat	**Incident**	Asset
DDoS attack on the central system	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data
Tampering with all or most control data in transit from the central system to the choke component	False control data received by all or most choke components	Provisioning of power to electricity customers
Tampering with data in transit from the metering terminal to the central system	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Same as the row above	Same as the row above
Metering node infected by malware	Malware compromises meter data	Integrity of meter data
Metering node infected by malware	Malware disrupts transmission of meter data	Availability of meter data
Metering node infected by malware	Malware disrupts the choke functionality	Provisioning of power to electricity customers
Tampering with control data in transit from the central system to the choke components for selected electricity customers	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers
Illegitimate control data sent to the choke components from the central system	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers

Consequences of Incidents

In order to estimate consequences, we need to consider the consequence scale for the identified asset

Table 6.5 Consequence scale for availability of meter data

Consequence value	Description
Insignificant	Meter data for up to 1,000 electricity customers unavailable for 1-24 hours
Minor	Meter data for up to 1,000 electricity customers unavailable for more than 1 day or meter data for 1,001-10,000 electricity customers unavailable for 1-24 hours
Moderate	Meter data for 1,001-10,000 electricity customers unavailable for more than 1 day or meter data for more than 10,000 electricity customers unavailable for 1-24 hours
Major	Meter data for more than 10,000 electricity customers unavailable for 25 hours-7 days
Critical	Meter data for more than 10,000 electricity customers unavailable for more than 7 days

This require to estimate the expected time to detect and respond to an attack, as well as the number of affected electricity customers

Table 7.5 Incidents caused by malicious threats

Threat	**Incident**	Asset
DDoS attack on the central system	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data
Tampering with all or most control data in transit from the central system to the choke component	False control data received by all or most choke components	Provisioning of power to electricity customers
Tampering with data in transit from the metering terminal to the central system	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data
Malware to manipulate meter data is installed on the metering terminal through connection to the external meter	Same as the row above	Same as the row above
Metering node infected by malware	Malware compromises meter data	Integrity of meter data
Metering node infected by malware	Malware disrupts transmission of meter data	Availability of meter data
Metering node infected by malware	Malware disrupts the choke functionality	Provisioning of power to electricity customers
Tampering with control data in transit from the central system to the choke components for selected electricity customers	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers
Illegitimate control data sent to the choke components from the central system	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers

Consequences of Incidents

CONSIDERATIONS

- In the experience of the distribution system operator, which is supported by their internal investigation reports of the incidents, the DDoS attacks that have occurred before have never caused loss of availability for more than one day

- The number of electricity customers whose meter data becomes unavailable can, however, be higher than before, as the customer base has increased

- Based on this information we therefore assign the consequence estimate *Moderate* to the incident

Consequences of Incidents

Table 8.5 Likelihood and consequence for incidents caused by malicious threats

No.	Incident	Asset	Likelihood	Consequence
1	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data	Likely	Moderate
2	False control data received by all or most choke components	Provisioning of power to electricity customers	Unlikely	Critical
3	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data	Likely	Minor
4	Malware compromises meter data	Integrity of meter data	Rare	Moderate
5	Malware disrupts transmission of meter data	Availability of meter data	Rare	Moderate
6	Malware disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
7	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers	Rare	Insignificant
8	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers	Unlikely	Moderate

Consequences of Incidents

Table 8.6 Likelihood and consequence for incidents caused by non-malicious threats

No.	Incident	Asset	Likelihood	Consequence
9	Communication between the central system and the metering terminal is lost	Provisioning of power to electricity customers	Certain	Minor
10	Same as the row above	Availability of meter data	Certain	Insignificant
11	Software bug on the metering terminal compromises meter data	Integrity of meter data	Unlikely	Moderate
12	Software bug on the metering terminal disrupts transmission of meter data	Availability of meter data	Unlikely	Moderate
13	Software bug on the metering terminal disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
14	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Provisioning of power to electricity customers	Unlikely	Moderate
15	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Availability of meter data	Possible	Minor
16	The metering terminal goes down due to damage from lightning	Provisioning of power to electricity customers	Likely	Insignificant
17	Same as the row above	Availability of meter data	Likely	Insignificant

Risk Evaluation

STEP 4

Recap: Evaluation of Cyber-risk

4 main steps (not too much different from the general case)

Consolidation of risk analysis results

Evaluation of risk level

Risk aggregation

Risk grouping

Consolidation of Risk Analysis Results

The goal of this activity is to make sure that the correct risk level is assigned to each risk

The central question is not whether each likelihood and consequence estimate is correct, but rather whether the resulting risk level is correct

Examples:

Let us consider the risk “Malware compromises meter data”.

- we assigned likelihood *Rare* and consequence *Moderate*.
- According to the risk evaluation criteria defined in step 1 we get a risk level *Low*.
- Even if the likelihood is increased to *Unlikely*, the risk level will remain *Low*.
- Hence, for this risk, the distinction between these two likelihood levels is not essential for determining the risk level

Let us consider the risk “Mistakes during maintenance of the central system prevent reception of data from metering nodes”.

If we are uncertain whether the consequence should remain at *Minor* or perhaps be increased to *Moderate*, then we need to investigate the issue, as this would bring the risk level from *Low* to *Medium*

Consolidation of Risk Analysis Results

We also make sure to check whether there are any risks that are both malicious and non-malicious.

- This is typically the case if malicious and non-malicious threats can result in the same incident

In our case, this would mean that the same incident occurs in both malicious and non-malicious Table.

In such cases we need to check that the likelihood and consequence estimates are consistent, and that both the malicious and the non-malicious causes have been considered when estimating the likelihood

This can be easy to overlook since we are dealing with the malicious and non-malicious risks separately during much of the risk assessment

Evaluation of Risk Level

The risk level of each risk is determined by its likelihood and consequence according to the risk matrix. In our case, risk evaluation is performed simply by plotting each risk in the risk matrix

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical					
	Major					
	Moderate					
	Minor					
	Insignificant					

Table 8.5 Likelihood and consequence for incidents caused by malicious threats

No.	Incident	Asset	Likelihood	Consequence
1	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data	Likely	Moderate
2	False control data received by all or most choke components	Provisioning of power to electricity customers	Unlikely	Critical
3	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data	Likely	Minor
4	Malware compromises meter data	Integrity of meter data	Rare	Moderate
5	Malware disrupts transmission of meter data	Availability of meter data	Rare	Moderate
6	Malware disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
7	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers	Rare	Insignificant
8	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers	Unlikely	Moderate

k Level

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6				
	Moderate	4, 5	8		1	
	Minor				3	
	Insignificant	7				

Table 8.6 Likelihood and consequence for incidents caused by non-malicious threats

No.	Incident	Asset	Likelihood	Consequence
9	Communication between the central system and the metering terminal is lost	Provisioning of power to electricity customers	Certain	Minor
10	Same as the row above	Availability of meter data	Certain	Insignificant
11	Software bug on the metering terminal compromises meter data	Integrity of meter data	Unlikely	Moderate
12	Software bug on the metering terminal disrupts transmission of meter data	Availability of meter data	Unlikely	Moderate
13	Software bug on the metering terminal disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
14	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Provisioning of power to electricity customers	Unlikely	Moderate
15	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Availability of meter data	Possible	Minor
16	The metering terminal goes down due to damage from lightning	Provisioning of power to electricity customers	Likely	Insignificant
17	Same as the row above	Availability of meter data	Likely	Insignificant

‹ Level

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical					
	Major	13				
	Moderate		11, 12, 14			
	Minor			15		9
	Insignificant				16, 17	10

Risk Aggregation

During the evaluation we need to take into account that some risks may "pull in the same direction" to the degree that they should actually be evaluated as a single risk.

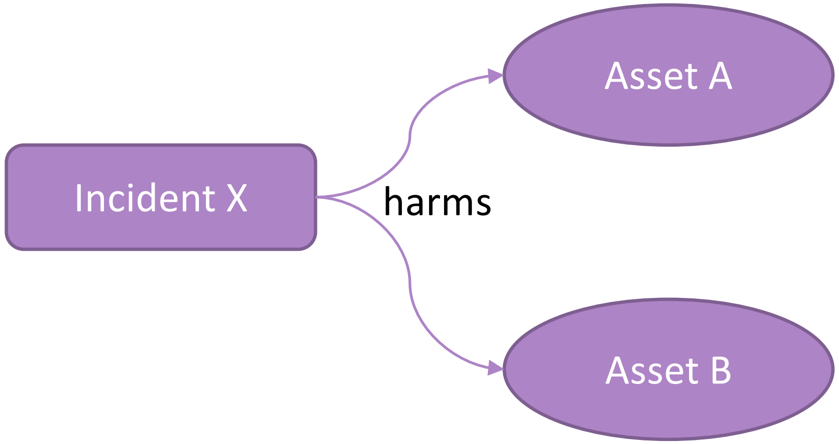
There are basically two cases where this may hold

CASE 1

Even if the risk of incident X harming asset A and the risk of incident X harming asset B are both low, it may be that the combined effect of harm to A and B warrants a higher risk level for the aggregation of these risks.

In this case

- the likelihood of the aggregated risks remains the same
- the consequence is the joint consequence of the two risks.



Risk Aggregation

During the evaluation we need to take into account that some risks may "pull in the same direction" to the degree that they should actually be evaluated as a single risk.

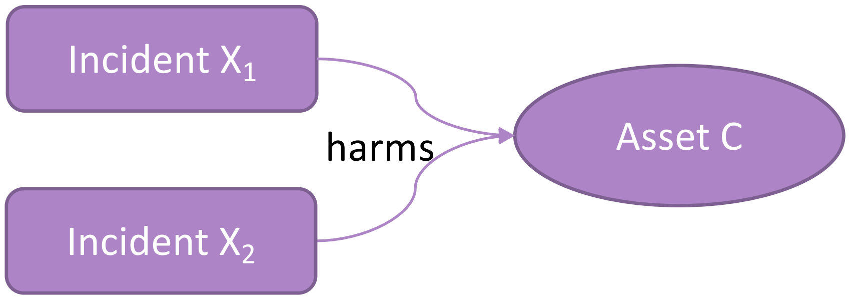
There are basically two cases where this may hold

CASE 2

Even if the risk of each individual incident harming the asset in question is low, it may be that the combined effect on the asset yields a higher risk.

A typical situation in which we might aggregate is when

- the incidents are of the same nature
- the occurrences of the incidents are triggered by the same threat.



Risk Aggregation

Going through Incident Tables, there are no instances where a single incident harms more than one asset.

Case 1 does not hold!

Table 8.5 Likelihood and consequence for incidents caused by malicious threats

No.	Incident	Asset	Likelihood	Consequence
1	Data from metering nodes cannot be received by the central system due to DDoS attack	Availability of meter data	Likely	Moderate
2	False control data received by all or most choke components	Provisioning of power to electricity customers	Unlikely	Critical
3	False meter data for a limited number of electricity customers received by the central system	Integrity of meter data	Likely	Minor
4	Malware compromises meter data	Integrity of meter data	Rare	Moderate
5	Malware disrupts transmission of meter data	Availability of meter data	Rare	Moderate
6	Malware disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
7	False control data received by the choke components for selected electricity customers	Provisioning of power to electricity customers	Rare	Insignificant
8	Power supply to electricity customers is switched off without legitimate reason	Provisioning of power to electricity customers	Unlikely	Moderate

Table 8.6 Likelihood and consequence for incidents caused by non-malicious threats

No.	Incident	Asset	Likelihood	Consequence
9	Communication between the central system and the metering terminal is lost	Provisioning of power to electricity customers	Certain	Minor
10	Same as the row above	Availability of meter data	Certain	Insignificant
11	Software bug on the metering terminal compromises meter data	Integrity of meter data	Unlikely	Moderate
12	Software bug on the metering terminal disrupts transmission of meter data	Availability of meter data	Unlikely	Moderate
13	Software bug on the metering terminal disrupts the choke functionality	Provisioning of power to electricity customers	Rare	Major
14	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Provisioning of power to electricity customers	Unlikely	Moderate
15	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Availability of meter data	Possible	Minor
16	The metering terminal goes down due to damage from lightning	Provisioning of power to electricity customers	Likely	Insignificant
17	Same as the row above	Availability of meter data	Likely	Insignificant

Risk Aggregation

However, risk no. 4, Malware compromises meter data, and risk no. 11, Software bug on the metering terminal compromises meter data, both concern software on the metering nodes and harm the integrity of meter data.

Case 2 hold

- they can therefore be viewed as special instances of a more generic incident, which we can call Software on the metering node compromises meter data.

Risk	Likelihood	Consequence
(4) Malware compromises meter data	Rare	Moderate
(11) Software bug on the metering terminal compromises meter data	Unlikely	Moderate
(4 + 11) Software on the metering node compromises meter data	Possible	Moderate

With similar considerations, it seems reasonable to aggregate risks nos. 5 and 12, and risks nos. 6 and 13. For the rest we decide to retain the original risks.

Risk Matrix after aggregation

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6, 13	(6+13)			
	Moderate		8, 11, 12, 14	(4+11), (5+12)	1	
	Minor			15	3	9
	Insignificant				16, 17	10

Risk Grouping

Observation: several risks may have benefit from the same treatment

In order to find out how to further group risks for our assessment, we systematically go through the results of the risk identification

Do any of these risks have anything in common that indicates that they will benefit from the same treatment?

Example

No.	Incident	Asset	Threat	Vulnerability
14	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Provisioning of power to electricity customers	Mistakes during update/maintenance of the central system	Poor training and heavy workload
15	Mistakes during maintenance of the central system prevent reception of data from metering nodes	Availability of meter data	Same as the row above	Same as the row above

Risk Grouping

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6, 13	(6+13)			
	Moderate		8, 11, 12, 14	(4+11), (5+12)	1	
	Minor			15	3	9
	Insignificant				16, 17	10

- Increasing the likelihood or consequence of either of them by a single step would bring its risk level to Medium.
- Treatments that address both these risks are therefore quite likely to be worth the cost.
- By grouping such risks we make it easier to take such considerations into account.

Risk Treatment

STEP 5

The final step of the cyber-risk assessment starts with identification of treatments for selected risks

We then assess the effect of the treatments and consider whether the residual risk is acceptable.

If it is, the documentation is finalized and the process terminates, otherwise we need to go back and do another iteration of the treatment identification.

Treatment Identification for malicious risks

Ideally, we would of course like to find treatments for all identified risks.

However, since we always have limited time and resources, we need to focus on those that are most important.

We therefore start by selecting risks based on the results of the risk evaluation.

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6, 13	(6+13)			
	Moderate		8, 11, 12, 14	(4+11), (5+12)	1	
	Minor			15	3	9
	Insignificant				16, 17	10

Treatment Identification for malicious risks

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6, 13	(6+13)			
	Moderate		8, 11, 12, 14	(4+11), (5+12)	1	
	Minor			15	3	9
	Insignificant				16, 17	10

Table 10.1 Malicious risks selected for treatment identification

No.	Risk level	Incident	Aggr.	Group
1	High	Data from metering nodes cannot be received by the central system due to DDoS attack	No	No
2	High	False control data received by all or most choke components	No	No
3	Medium	False meter data for a limited number of electricity customers received by the central system	No	No
4	Low	Malware compromises meter data	4+11	4,5,6
5	Low	Malware disrupts transmission of meter data	5+12	4,5,6
6	Low	Malware disrupts the choke functionality	6+13	4,5,6

Treatment Identification for malicious risks

The next step is to identify treatments for the selected risks.

For each risk we therefore create a small table summarizing relevant information for the treatment

Element	Description
Risk n.	
Incident	
Asset	
Threat Source	
Threat	
Attack Point	
Vulnerability	
Treatment	

Treatment Identification for malicious risks

Element	Description
Risk n.	1
Incident	Data from metering nodes cannot be received by the central system due to DDoS attack
Asset	Availability of meter data
Threat Source	Script kiddie; Cyber-terrorist
Threat	DDoS attack on the central system
Attack Point	Internet connection to the central system
Vulnerability	Inadequate attack detection and response on central system
Treatment	Implement state-of-the-art DDoS attack detection and response mechanism on central system

Risk Acceptance

Implementing treatments always carries a cost

For each treatment we therefore need to weigh its effect against its cost

We first estimate the effect of a treatment in terms of reduced risk level for the affected risks, before estimating its cost

Quantitative vs Qualitative

Cost-Benefit Analysis

Risk	Data from metering nodes cannot be received by the central system due to DDoS attack
Risk Level	High
Treatment	Implement state-of-the-art DDoS attack detection and response mechanism on central system

Considerations

- Implementing the treatment will hardly prevent script kiddies or cyber-terrorists from launching DDoS attacks -> No effect on the threat
- However, early detection will reduce the likelihood that the attack actually leads to the incident in question -> Likelihood moves from Likely to Possible
- a prompt response implies that fewer electricity customers are affected, and that they are affected for a shorter period -> Consequence moves from Moderate to Minor
- The overall risk level decreases from High to Low

Cost-Benefit Analysis

Risk	Data from metering nodes cannot be received by the central system due to DDoS attack
Risk Level	High
Treatment	Implement state-of-the-art DDoS attack detection and response mechanism on central system

Considerations

- the treatment requires a significant investment in hardware and network infrastructure
- Arriving at an adequate set of detectors (preferably combining anomaly-based and signature-based approaches) will take time and effort.
- The cost of the treatment is therefore High.

Cost-Benefit Analysis

Iterating over the risk we got the following table

Table 10.7 Effect of treatments

Treatment	Risk	Effect	Cost
Implement state-of-the-art DDoS attack detection and response mechanism on central system	1	High to Low	High
Stronger integrity checking of received meter data on central system	4 11 4+11	Low to Low Low to Low Medium to Low	High
Hire more staff	14,15	Low to Low	High
Develop executable scripts for routine maintenance tasks	14,15	Low to Low	Low