Chapter 7
Risk Identification

After establishing the context, we are ready to start identifying risks. Here the goal is to arrive at a collection of threat sources, threats, vulnerabilities, incidents, and risks that is as correct and complete as possible for our particular target of assessment and assets. We start by giving an overview of some risk identification techniques, before moving on to identification of risks caused by malicious threats, as described in Sect. 5.3.2, and risks caused by non-malicious threats, as described in Sect. 5.3.3.

7.1 Risk Identification Techniques

Since cyber-systems are computer based, there is normally a lot of data and information available from event logs, intrusion detection systems and other monitoring tools, vulnerability scanners, results from penetration tests or other kinds of security tests, source code reviews, and so on. When identifying risk we try to fully exploit such information. Therefore we perform a systematic walk-through of the target description, including the attack surface and assets, in order to identify any such information sources to be used. These sources are mapped to the relevant part(s) of the target, which will also be useful in the risk analysis step later. Typically, this is done in close cooperation with maintenance personnel, technical managers, security managers, or others who have detailed knowledge about the technical infrastructure. For example, any test results concerning the metering terminal interface to the Internet are mapped to this particular part of the attack surface. These test results then help us to identify vulnerabilities and threats for attacks through this interface. Table 7.1 illustrates a simple way of documenting this kind of information. The first column shows which part of the target system, attack surface, or asset the information relates to. The second column briefly describes the kind of information and source, while the third column provides a reference to the source.

Notice that, 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. Even if a certain threat has not materialized in the past, it does not mean that it cannot do

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_7

Table 7.1 Results from tests, monitoring logs, and so on of relevance to risk identification

Part of target / asset	Source description	Reference
Connection point between metering terminal and external meters	A test of the metering terminal interface to external meters was performed last year. The test included checking whether there is adequate input sanitation. A written report documents the test procedure and results.	MeterTest.docx
Availability of meter data	The central system logs all instances of meter data from the metering node of an electricity customer not being received at the expected point in time. The logs for the last three-year period have been compiled in a single pdf file.	MissingMeterData.pdf

so in the future. The absence of corresponding events from the logs does not mean that a threat or incident should be left out of the assessment. This is particularly important to remember with respect to rare incidents with a high consequence, such as a large-scale coordinated attack on the metering infrastructure. Similarly, even if a vulnerability is not detected by a security test, it does not mean that it does not exist. For the risk identification we need not consider the severity of vulnerabilities or the likelihood of threats and incidents; at this point we document everything that may be relevant and leave the further analysis for later.

Throughout the risk identification, and also during the risk analysis later, we make sure to carefully consider whether there are parts of the target for which more security testing, logging/monitoring, or other probing is needed. This is, however, also a question of available time and resources. Furthermore, it depends on whether the required information can be obtained by other means.

In addition to the target-specific information sources discussed above, valuable input to the risk identification can also be found in open sources such as international standards, online repositories, and various reports on cybersecurity, threats, and vulnerabilities. When exploiting such input, our main challenge is to identify the specific sources of relevance, and to select from these sources only those elements that are relevant to our assessment. Here we recommend a simple four-step approach:

1. Establish relevance criteria based on, for example, the kind of system or domain you are dealing with, the assets, or the risk type.
2. Identify information sources based on the established criteria. For an overview of open sources of information, see Chap. 5. We also give some examples of references regarding specific parts of the risk identification process throughout this chapter.
3. Select from these sources only those elements that are relevant to your assessment.
4. Reformulate the selected elements, which by necessity are described in general terms, so that they apply specifically to your target of assessment and assets.

Even if we are dealing with cyber-systems, it is essential for the risk identification to extract information not only from system logs, security tests, and so on, but also from people who know the target of assessment well from their particular viewpoints. For our assessment, these people may include the developers of the central system or metering nodes, the maintenance team and operators of the central system, the information security officer and managers of the distribution system operator, and potentially also some of their electricity customers.

External experts may also possess valuable knowledge for our assessment; although they do not know the specific target of assessment, they may provide general information about typical threat sources, vulnerability and attack types, and trends. When interacting with external experts you must of course take great care not to disclose confidential information unless this has been approved by the party on whose behalf we conduct the assessment.

For obtaining information from people, we may employ interviews. Interviews can follow a strict structure where all questions are planned in advance, but we can also use an open format with key themes to be covered, yet with considerable openness to additional inputs from the interviewee. The most appropriate option is usually a mixed approach where we prepare questions, but are ready to follow up on any unforeseen but relevant issues that the interviewee brings up. Interviews may provide very valuable information, but must be used with care. Interviews are quite resource intensive and depend on the right persons being willing and available. Carrying out the interviews and compiling and aggregating results also require skill from the risk assessors.

Another option for extracting information and knowledge from people is the use of questionnaires. This is easier to organize than interviews, as we do not have to agree with the subject on a date. On the downside, we lose the possibility of asking follow-up questions or making clarifications. Moreover, the subject has little opportunity to elaborate on issues that are not covered by the questionnaire, meaning that we may lose important information.

We can also make use of brainstorming and similar techniques for risk identification. This involves gathering together relevant stakeholders and personnel with first-hand knowledge about specific parts or aspects of the target to contribute to the identification process in plenary sessions. A big advantage of this approach is that the participants are able to discuss and to follow up on each other's ideas. For example, if one participant identifies a vulnerability not thought of by anyone else, then all of them can think of ways in which threats can exploit this vulnerability. Assuming we are able to gather the right people, this can potentially prove very successful. Unfortunately there are also some pitfalls associated with brainstorming that we need to keep in mind. One is that the personalities of the participants play a major role, and there is a danger that the more outspoken persons dominate while others hardly contribute, so that not all views are brought forward. Individual participants may also take the opportunity to pursue their own agenda and focus only on issues that are within their own area of interest. Other pitfalls are that the discussion can digress off topic and that the available time may not be properly distributed between the topics to be covered.

Successful brainstorming therefore requires a highly skilled risk assessor to lead the sessions. It also requires that we make plans in advance for how to structure and guide the discussions. The structure can be based on, for example, assets, threat source types, vulnerability types, or parts of the target description or attack surface. How we choose to structure the brainstorming is up to us, but in general it depends on the target of assessment, any preferences of the participants, and which step of the risk identification we are dealing with. How to do on-the-fly documentation of the proceedings may also pose a challenge. We therefore need to appoint a dedicated secretary with this responsibility. If all participants consent, we could of course use video or audio recordings, but we do not generally recommend this, as it is likely to inhibit the participants. On the more practical side, gathering together all the participants for a brainstorming session may also be difficult.

Which information sources and techniques to use for the risk identification depends on a number of factors, such as available resources and information sources, and the kind of target. For example, for a standard web application or service of a non-critical system, a satisfactory risk identification can probably be based to a large degree on generic standards and repositories of cyber-threats and vulnerabilities. On the other hand, when dealing with a highly specialized critical system such as the AMI, the risk identification is much more involved. We therefore seek to combine techniques to get as complete a picture as possible and to confirm the results. For example, if interviews reveal uncertainty about the presence of certain kinds of vulnerabilities or the feasibility of attacks, then vulnerability scanning and security testing can help to reduce the uncertainty.

For documenting and structuring risk assessment results, in Part II of this book we employ tables and textual descriptions. We consider tables to be well suited for our purposes since the assessment will be done at a generic level, without going deeply into the technical details of how threats and incidents materialize. Common alternatives to tables are various kinds of graph-based risk-modeling techniques. For an overview of risk-modeling techniques and their area of use, see ISO/IEC 31010 [30].

7.2 Malicious Risks

As explained in Sect. 5.3.2, when identifying malicious risks we basically need to understand how a game between an adversary and the defender may play out. How the adversary may launch attacks, which vulnerabilities he or she may exploit, and what incidents may result if the attack succeeds depend on who the adversary is. Therefore we start by identifying relevant adversaries, which we refer to as threat sources. Then we move on to threat identification, where we describe potential attacks with respect to the assets in question, before identifying vulnerabilities, and finally incidents.

Notice that although this order offers a good way to structure the identification process, it only serves as a guideline. We are free to deviate whenever it serves the

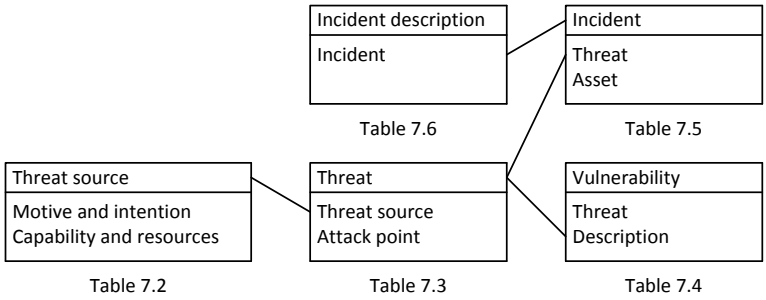

Fig. 7.1 Overview of tables documenting risks caused by malicious threats

overall goal and to go back and update previous results at any time. For example, if a constructive discussion about vulnerabilities starts during the threat source identification, then we make sure to document all relevant comments, and go back to the threat sources later. The important thing is to establish a collection of relevant threat sources, threats, vulnerabilities, incidents, and risks that is both consistent and as complete as possible. The results we present in this chapter show the final outcome of the identification process.

Figure 7.1 gives an overview of the tables that we use to document risks caused by malicious threats, as well as the relations between these tables. Each box represents a table. The uppermost compartment shows the main column, the heading of which occurs in boldface in the actual table. The lowermost compartment represents the rest of the columns. Lines between tables indicate entries that occur in more than one table. For example, threats occur also in the vulnerability table since vulnerabilities are considered in relation to threats. The table number is indicated below each box. As we will explain in the following, the tables are designed to accommodate the risk identification approach. The risks may be deduced implicitly. For each pair of an incident and asset harmed by the incident there is one risk.

7.2.1 Threat Source Identification

To identify malicious threat sources we need to understand who may want to initiate attacks and why. For this purpose we consider all possible motives and intentions, including financial gain, revenge or grudges, political or religious agendas, espionage, or simply fun and a desire to prove one's ability. The potential for causing harm will to a large degree depend on the motive and intention of the threat sources, as well as their capabilities and available resources. It is therefore important to document these characteristics in the threat source descriptions, and we have designed Table 7.2 accordingly. For this assessment we have chosen to use free text to capture threat source characteristics. This will provide valuable input to the analysis of likelihood and consequence later. Alternatively, we could have defined quantitative

or qualitative scales, in the same way as we did for likelihood and consequence of incidents during the context establishment. See Chap. 11 for a further discussion of this approach.

Information sources of potential relevance include the ISO 27005 standard [32] and the report on critical infrastructure protection from the United States Government Accountability Office (GAO) [81]. The former lists, among other things, human threat sources and their motives. The latter lists malicious sources of cybersecurity threats in the context of critical infrastructure protection. Although written from a US perspective, this generic list is equally relevant worldwide, as cyber-threats know no borders. Another source is the NIST guide for conducting risk assessments [54], which lists a number of malicious threat sources.

Table 7.2 documents the malicious threat sources that we identified for the assessment of the smart grid AMI based on the target and the gathered data. Notice that although the descriptions in the table are quite generic, we have selected each of them because they are of relevance to our specific target of assessment, as this is a potential target for their attacks. Understanding how these threat sources can cause concrete threats is the task of the subsequent identification of malicious threats. Before moving on to that we explain the reasoning behind the inclusion of some of the documented threat sources to illustrate the approach.

Script kiddie: Attacks on power supply systems may potentially get a lot of media attention, as power supply concerns everyone. This applies not only to the provisioning of power, but also to corresponding billing and payment services. Such systems may therefore be attractive targets for script kiddies seeking attention.

Cyber-terrorist: A power supply system is a critical infrastructure. Blackouts and disruptions can have huge societal consequences in any modern society. Power supply systems are therefore highly attractive targets for cyber-terrorists seeking to disrupt society or cause societal crises or emergencies.

Black hat hacker: The billing and payment of electric power involve high economic values. A black hat hacker able to tamper with power consumption data could for example use this ability to offer an "electric power bill reduction service" on the black market.

7.2.2 Threat Identification

For each malicious threat source we identify the threats it may initiate. Table 7.3, which documents malicious threats, therefore includes a *Threat source* column as well as the *Threat* column. In addition, for this task we focus specifically on how the threat sources may exploit the attack surface identified during the context establishment. Therefore we also include a separate *Attack point* column to show which parts of the attack surface are being exploited by each threat. By including these three elements in the table format, we also document the explanation behind the identified threats. This is necessary both for the later risk analysis and for the final reporting of the risk assessment results.

Table 7.2 Malicious threat sources

Threat source	Motive and intention	Capability and resources
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
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
Black hat hacker	Motivated by personal gain, for example through tampering with data or blackmail. This includes, for example, electricity customers who seek to reduce their electricity bill by tampering with meter data	The skill level of black hat hackers can vary a lot, but the best are world-leading experts on cybersecurity. If part of a larger criminal organization, they can also command significant resources
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
Insider	An insider is a disloyal employee or consultant of the distribution system operator who is typically motivated either by personal gain or by a desire to harm the employer due to conflicts and discontent	May have access to all systems and possess detailed information and knowledge about the system architecture, functionality, and security features
Malware	By malware we mean here malicious software developed to harm computerized systems, but which are not aimed specifically at harming the assets of the party of the risk assessment	Developers of malware are often highly skilled. Malware can therefore cause significant harm to systems based on standard off-the-shelf operating systems or other software

Again, the examples of typical threats provided by ISO 27005 offer useful input for the threat identification. Other examples include the section on attack mechanisms in ISO 27032 [28], the attack vector descriptions provided by the OWASP top 10 [63], and the representative examples of malicious threats found in the NIST guide for conducting risk assessments [54]. CAPEC [51] also offers an online database of cyber-attack patterns.

Descriptions in sources such as the above are, of course, not specific to our target of assessment. We therefore make sure to describe each of the relevant threats as it applies to our particular target. Table 7.3 documents the results, some of which we explain further below.

DDoS attack on the central system: Regarding script kiddies we consider DDoS attacks as a potential threat, as DDoS attacks have been well known for a long time and a lot of information about how to launch such attacks is available online. It is also possible to buy services for such attacks on the black market. DDoS attacks are also a relevant threat with respect to cyber-terrorists, who may launch such attacks in an attempt to disrupt power provisioning.

Tampering with all or most control data in transit from the central system to the choke component: This threat can be initiated by a cyber-terrorist attack in order to disrupt the power supply. As control data from the central system can be used to choke or disconnect power for electricity customers, tampering with such data for a large number of customers can cause significant societal disruption, which can be a goal for cyber-terrorists. The control data are sent over the Internet. Tampering with data in transit therefore represents a relevant threat for our assessment.

Malware to manipulate meter data is installed on the metering terminal through connection to the external meter: Black hat hackers can potentially make a profit from manipulation of meter data. One way to achieve this is to install malware on the metering terminal, so that manipulated data are sent to the central system. The metering terminal is often connected to external meters, and such connections represent a potential attack point for installation of malware.

7.2.3 Vulnerability Identification

For each malicious threat we identify the existing vulnerabilities that the threat may exploit. Table 7.4, which documents these findings, therefore includes a *Threat* column as well as the *Vulnerabilities* column. We also include a *Description* column, which allows us to provide a more extensive description of the vulnerability. During the identification we pay special attention to the attack point documented as part of the threat identification, as well as any weaknesses of defense mechanisms, or lack of such mechanisms.

With respect to exploiting external information sources, a full chapter of the NISTIR 7628 guidelines for smart grid cybersecurity [53] is dedicated to listing vulnerabilities, divided into four classes: 1) people, policy, and procedure; 2) platform software/firmware vulnerabilities; 3) platform vulnerabilities; and 4) network. ISO 27005 offers a list of vulnerabilities related to hardware, software, network, personnel, site, and organization. Other sources of general vulnerabilities include the online resources offered by OWASP [61] and the common weakness enumeration offered by MITRE [52].

In addition to exploiting such sources, we also take advantage of the fact that our target of assessment is an executing system that can be subject to vulnerability

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

scanning and other forms of security testing. This helps us to check whether suspected vulnerabilities are actually present, and may also reveal new vulnerabilities. The use of tests for identification of vulnerabilities should of course be documented. This could, for example, be done by including a separate column with a reference to related tests and test results for each vulnerability. We have chosen not to include such a column here, as going further into the actual tests would be beyond our scope. Table 7.4 documents the results of the identification of vulnerabilities with respect to malicious threats.

Inadequate attack detection and response on central system: Successful protection against DDoS attacks requires firstly that the system is able to detect the attack and secondly that an adequate defense can be initiated. The attack detection mechanism on the central system may, however, be outdated. It may not be clear whether it is able to catch the more advanced kinds of DDoS attacks we have seen in recent years; hence, this needs further investigation. The response is based purely on dropping packets according to fixed classification rules and gives little opportunity for analysing the attack.

Weak encryption and integrity check: Concerning all the identified threats involving tampering with data in transit, members of the central system maintenance team had concerns with the encryption strength of meter data and control data. Hence, this is a potential vulnerability that needs further investigation. The same applies to the integrity checking of such data.

Unprotected local network, no sanitation of input data from the external meter: With respect to the threat of malware being installed on the metering terminal through the connection to the external meter, a test of this interface indicated that there was no sanitation of input to the metering terminal from external meters, which leaves this component vulnerable to injection attacks. This is particularly worrying since the distribution system operator has no means to ensure the protection of the electricity customer's local network over which the metering terminal communicates with the external meter.

Notice that some approaches prescribe the identification of controls or barriers, which are means to prevent threats occurring and/or leading to incidents. For our assessment we consider this to be covered by the vulnerability identification, in the sense that a weak or nonexistent control/barrier constitutes a vulnerability. For example, encryption can be used as a barrier against confidentiality breaches. Weak encryption, for example due to a weak cryptographic hash function or poor protection of keys, will therefore constitute a vulnerability.

7.2.4 Incident Identification

Before moving on to the risk analysis step we need to identify the incidents that may result from the threats and actually harm our assets. In other words, we need to think of potential ways that our assets can be harmed by the threats. Table 7.5, which documents incidents, therefore contains a *Threat* column and an *Asset* column in addition to the *Incident* column. Vulnerabilities are of course also considered, but have not been included in this table, as they are already related to the threats in Table 7.4. Notice that Tables 7.2, 7.3, 7.4, and 7.5 together provide information about each complete chain consisting of a threat source, threat, vulnerability, incident, and affected asset. As mentioned above, for each pair of an incident and asset harmed by the incident there is a risk.

The general information sources we consult to identify incidents are to a large degree the same as we used for threats and vulnerabilities. For example, the list of threats provided by ISO 27005 [32] also includes information about incidents that may result from the threats, such as unauthorized system access and system tampering. OWASP [63] descriptions include information about results of attacks, such as denial of access, user sessions being hijacked, and so on. The attack pattern enumeration offered by MITRE [51] also provides similar descriptions. As in the case of vulnerabilities, security testing can also be used to gain a better understanding of potential incidents.

When exploiting general information sources such as those mentioned above, we make sure to tailor the descriptions so that every incident is clearly expressed in a way that relates specifically to our particular target of assessment and assets. Table 7.5 documents the results of the identification of incidents resulting from malicious threats. The descriptions are given at a high level of abstraction, which is in

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
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

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

line with the directions given by the distribution system operator during the context establishment. Below we explain the reasoning behind some of the entries.

Data from metering nodes cannot be received by the central system due to DDoS attack: This incident may result from a DDoS attack on the central system, since a successful attack will keep this system too busy serving illegitimate requests. This means that meter data becomes unavailable to the distribution system operator, at least temporarily.

False control data received by all or most choke components: Clearly, tampering with all or most control data in transit from the central system to the choke component may lead to this incident, as the control data will not constitute authentic data sent from the central system. Since the threat source in this case is a cyber-terrorist, it is likely that the control data will be manipulated so as to disrupt the provisioning of power to the electricity customers.

False meter data for a limited number of electricity customers received by the central system: This incident may result from tampering with data in transit from the metering terminal to the central system, which is a threat initiated by a black

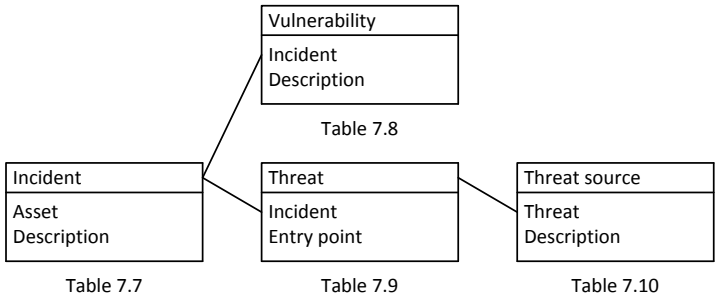

Fig. 7.2 Overview of tables documenting risks caused by non-malicious threats

hat hacker. Reception of false meter data would of course harm the integrity of the meter data.

Often it is useful to provide more information about identified incidents than what is offered by Table 7.5. We therefore include further descriptions in Table 7.6.

7.3 Non-malicious Risks

As explained in Sect. 5.3.3, for risks where no malicious intent is involved, we start from the assets in order to guide the identification process and ensure that we maintain the right scope. The first step is to identify accidental incidents that may harm the assets. Only threats, vulnerabilities, and threat sources that relate to such incidents are relevant. Starting with identification of incidents therefore helps us to focus the rest of the process on the important elements. Having identified non-malicious incidents, the next steps are to identify the weaknesses of the target that make the incidents possible, that is to say the vulnerabilities, and the threats that may lead to the incidents. Finally, we identify the threat sources that can initiate these threats. Similarly to the case of malicious risks, the above order provides a useful guideline for structuring the identification, although we allow ourselves to deviate from this order whenever appropriate. The results we present show the final outcome of the process.

Figure 7.2 gives an overview of the tables that we use to document risks caused by non-malicious threats. They are designed to support the identification process outlined above, but are sufficiently flexible to also accommodate other approaches.

Table 7.6 Further description of incidents caused by malicious threats

Incident	**Incident description**
Data from metering nodes cannot be received by the central system due to DDoS attack	This refers to incidents resulting from all kinds of DDoS attacks that target the central system and prevent it from receiving data from power meters. Such an attack will typically be performed by saturating the central system with communication requests, for example by distributed botnets posing as legitimate power meters
False control data received by all or most choke components	This refers to incidents resulting from large-scale tampering with control data in transit from the central system. As control data to choke components control the amount of power available to an electricity customer, such threats can lead to widespread brownouts or even blackouts. In order to succeed in sending false messages, an attacker must get into the communication path, intercept and modify legitimate messages or create new messages, and ensure that that the modified or new messages are considered valid by the choke components. However, if the default action of these components is to switch off in the absence of valid control data, then a blackout can be achieved simply by preventing legitimate messages from reaching the choke components
False meter data for a limited number of electricity customers received by the central system	This refers to such incidents resulting from either tampering with meter data in transit from metering terminals or malware on the metering terminals. The technical ways in which the former may be achieved is similar to the previous case. However, as data from metering nodes to the central system primarily concern power consumption, the motive would most likely be financial gain. A black hat hacker could for example offer to manipulate data in order to reduce electricity bills for a suitable fee
Malware compromises meter data	Metering terminals connected to the Internet may be infected by malware even if no malicious person has physical access, thereby affecting their ability to correctly register meter data
Malware disrupts transmission of meter data	Similarly to the case above, malware may affect the ability of the metering terminal to correctly transmit meter data to the central system
Malware disrupts the choke functionality	As the choke component receives control data from the central system via the metering terminal, malware on the metering terminal may prevent it from forwarding correct control data to the choke component. It is also possible that the choke component itself is infected by malware via the metering node
False control data received by the choke components for selected electricity customers	This refers to the same kind of incident as described for *False control data received by all or most choke components* above, except that only a small group is targeted. This would require attackers to be able to identify the specific control signals going to the target group, but is otherwise similar to the above case
Power supply to electricity customers is switched off without legitimate reason	This refers to cases where an insider does this on purpose. This would be a breach of operating procedures and require that the insider knows how to operate the control signals from the central system, but would not otherwise require any specialized cybersecurity or programming skills

7.3.1 Incident Identification

In order to identify incidents caused by non-malicious threats we start from the assets by considering how these can be harmed. Table 7.7, which documents the identified incidents, therefore includes an *Asset* column in addition to the *Incident* column. We also include a *Description* column which allows us to provide further explanation of each incident.

When identifying incidents we pay special attention to the way the assets relate to or are represented in the system. With respect to integrity and availability of meter data, we notice that an electricity customer's power consumption is read by the power meter and fed to the metering terminal, which transmits meter data to the central system over the Internet. Incidents can therefore affect these assets all along this chain. For provisioning of power to electricity customers, control data are sent from the central system to the metering terminal and forwarded to the choke component. Depending on the received data, this component may switch off or reduce the amount of power provided to the customer. To aid the identification of incidents, we make use of sources such as system logs, monitored data, repositories of previous incidents or other historical data, and input from people with knowledge about the target system. Table 7.7 documents incidents caused by non-malicious threats. In the following we explain the reasoning behind the inclusion of some of the rows to illustrate the approach.

Communication between the central system and the metering terminal is lost: If this communication is broken then the choke component will not receive control data from the central system, which disrupts the provisioning of power. In addition, the central system will not receive meter data from the metering terminal.

Software bug on the metering terminal compromises meter data: Transmission of correct meter data depends on the correct functioning of the metering terminal. A software bug may cause a malfunction that can potentially result in corrupted meter data being sent to the central system, thereby compromising the integrity of these data.

Mistakes during maintenance of the central system disrupt transmission of control data to the choke component: Provisioning of power may be disrupted if correct control data are not received by the choke component. This means that misconfiguration of communication parameters or other maintenance mistakes that disrupt transmission of control data may also disrupt power provisioning.

The metering terminal goes down due to damage from lightning: If the metering terminal goes down then it will not be able to transmit meter data or receive control data. This incident will therefore harm availability of meter data and provisioning of power to the affected electricity customers.

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

7.3.2 Vulnerability Identification

For each identified incident we look for vulnerabilities that allow the incident to occur or that increase its likelihood. Table 7.8, which documents vulnerabilities with respect to non-malicious incidents, therefore includes an *Incident* column in addition to the *Vulnerability* column. We also include a *Description* column to provide more information about the vulnerability.

Vulnerabilities with respect to non-malicious threats are often related to the ability of operators or other persons interacting with the system to perform their tasks as expected. We therefore pay special attention to human, social, and organizational factors such as training, skills, time pressure, and procedures. For our assessment this applies, for example, to those who operate and maintain the central system. Similar considerations also apply to suppliers on whose services or products the system

depends. We also consider the technical vulnerabilities of software, hardware, and other equipment that affect our target of assessment. The sources of vulnerability descriptions to be found in the literature are largely the same as for the malicious case, although the relevant entries may of course differ.

Table 7.8 documents the results of the identification of vulnerabilities with respect to non-malicious threats. The reasoning is explained below.

Single communication channel between central system and metering terminal: Many electricity customers do not have the possibility of communication via GPRS and rely solely on the Internet connection. This is an obvious weakness with respect to maintaining communication.

Poor testing: This vulnerability applies to the software of metering terminals, which run quite complicated software. This software is responsible for registering power readings from the power meter and transforming these readings into meter data to be submitted to the central system. It is also responsible for receiving control data from the central system and forwarding these to the choke component. In addition, there are the general protocols and functionality for communication with the central system and external components such as the controlled unit. Extensive testing according to state-of-the-art methods is therefore required.

Poor training and heavy workload: This applies to members of the maintenance team responsible for the central system, which is the single most important component of our target of assessment. Maintenance of the central system is very difficult, as it consists of a number of hardware and software components, communicates with other systems, and needs to run continuously. A log of previous errors raises doubts about whether all members of the maintenance team have the required skills and experience. The experienced members of the maintenance team have a very heavy workload and may not always be available when needed.

Inadequate overvoltage protection: Metering terminals include computing hardware that is not very robust with respect to transient overvoltages, for example caused by lightning. It is doubtful whether the overvoltage protection of most electricity customers provides the required level of protection.

7.3.3 Threat Identification

Having identified vulnerabilities for each incident, we move on to identify the threats that may, due to the vulnerabilities, cause the incidents to occur. Each threat is related to (at least) one incident and corresponding vulnerability. To link the threats to incidents, we include an *Incident* column as well as a *Threat* column in Table 7.9, which documents non-malicious threats. Moreover, we go through the target description to find parts or components where threats may occur. To document this we also include an *Entry point* column. Table 7.9 documents the results of the non-malicious threat identification.

Internet connection to the metering terminal goes down: Given the vulnerability of a single communication channel between the central system and the metering

Table 7.8 Vulnerabilities with respect to non-malicious threats

Incident	**Vulnerability**	Description
Communication between the central system and the metering terminal is lost	Single communication channel between central system and metering terminal	For many electricity customers there is no redundant communication link to the central system
Software bug on the metering terminal compromises meter data	Poor testing	The software for the metering terminals is developed and tested by the metering terminal supplier. Previous experience indicates that their testing routines are not satisfactory
Software bug on the metering terminal disrupts transmission of meter data	Same as the row above	Same as the row above
Software bug on the metering terminal disrupts the choke functionality	Same as the row above	Same as the row above
Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	Poor training and heavy workload	Maintenance of the central system is highly challenging due to its complexity and the need to operate 24/7. Hence, performing these tasks requires extensive training and experience. The persons that have the required skills also have a heavy workload, meaning that less qualified personnel sometimes need to carry out the tasks
Mistakes during maintenance of the central system prevent reception of data from metering nodes	Same as the row above	Same as the row above
The metering terminal goes down due to damage from lightning	Inadequate overvoltage protection	Robust overvoltage protection is needed to protect the metering terminals from lightning

terminal for many electricity customers, it is clear that communication will be lost if the metering terminal loses its Internet connection.

Buggy software distributed on metering terminals: We have identified three incidents involving software bugs, and poor testing has been shown to be a vulnerability. Distribution of buggy software is therefore an important threat to consider.

Mistakes during update/maintenance of the central system: Two of our incidents concern mistakes during update/maintenance of the central system. Such mistakes therefore constitute a relevant threat, in particular in the light of poor training and heavy workload having been identified as a vulnerability.

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

7.3.4 Threat Source Identification

It now remains to identify threat sources. For each threat we ask what its potential source can be. Table 7.10, which documents non-malicious threat sources, therefore includes a *Threat* column as well as the *Threat source* column. An additional *Description* column lets us provide extra information about the threat source.

When identifying non-malicious threat sources we focus on technical errors occurring in the target of assessment or in systems on which it depends, persons that may make mistakes or behave in unforeseen ways when legitimately interacting with the target, and natural phenomena such as lightning and flood. As an aid in this task, ISO 27005 [32] provides a nice overview of potential threat sources, divided into categories such as physical damage, natural events, and technical failures. In addition, NIST [54] provides lists of non-malicious threat sources divided into the categories accidental, structural, and environmental sources. Potential threat sources that we need to consider for our assessment include, for example, those who operate and maintain the central system, software and hardware components on the side of the distribution system operator and the electricity customer, and all communication links. Table 7.10 shows the result of the identification of non-malicious threat sources.

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

7.4 Further Reading

An overview of vulnerabilities for smart grids can be found in the guidelines for smart grid cybersecurity from NIST [53]. In their recommendations for protecting industrial control systems, ENISA gives a high-level view of the current situation of technological threats with respect to protecting such systems [14]. EUROPOL [16] provides an assessment of Internet organized-crime threats from a European police perspective. The document includes a section on vulnerabilities of critical infrastructure that specifically addresses smart grids. Although threats are described at a very generic level, documents like this can add a useful perspective to the risk identification. For an overview of general threats, vulnerabilities, and other information not specifically addressing smart grids or other critical infrastructures, we refer to Sect. 5.5. With respect to combining risk analysis and testing, the OWASP testing guide [64] provides some discussion of the relationship between security testing and risk analysis. There is also an emerging field of research in this area that will hopefully mature further in the near future [10, 11, 21].