Towards Improved Understanding and Holistic Management of the Cyber Security Challenges in Power Transmission Systems

Inger Anne Tøndel, Bodil Aamnes Mostue, Martin Gilje Jaatun, Gerd Kjølle

Towards improved understanding and holistic management of the cyber security challenges in power transmission systems

Inger Anne Tøndel[1], Bodil Aamnes Mostue[2], Martin Gilje Jaatun[1], and Gerd Kjølle[3]

[1] SINTEF ICT, Trondheim, Norway
inger.a.tondel@sintef.no
[2] SINTEF Technology and Society, Trondheim, Norway
[3] SINTEF Energy Research, Trondheim, Norway

Abstract. Information and Communication Technology (ICT) is increasingly utilised in the electrical power transmission system. For the power system, ICT brings a lot of benefits, but it also introduces new types of vulnerabilities and threats. Currently the interdependencies between the power and ICT system are not fully understood, including how threats (both malicious and accidental) towards the ICT system may impact on power delivery. This paper addresses the need for improved understanding between ICT security and power experts. It explains important terms used differently in the two disciplines, identifies main impacts on power systems that may result from ICT incidents, and proposes a set of indicators that can be used as a basis for selecting measures.

Keywords: information security, cyber security, power transmission, indicators

1 Introduction

The next-generation electric power system (the smart grid) is central in dealing with emerging energy challenges. In Europe, the goal of 20 % improvement in energy efficiency, 20 % share of renewable energy, and 20 % reduction in greenhouse gas emissions by 2020 is a driver towards a smarter grid where renewable energy can be more effectively introduced, failures can be more easily detected and managed and where customers and their smart appliances consume energy in a more flexible way.

The electric power system can be divided into three main areas: *Generation* of energy, *transmission* of energy at high voltage over long distances, and *distribution* of energy at lower voltage towards customers. The transmission system is already quite smart compared to the distribution system, and most of the smart grid initiatives thus introduce more intelligence into the distribution grid. Advanced Metering Infrastructure (AMI) is one such modernisation.

For power systems, the N-1 principle has guided the work on securing the infrastructure; the power system should withstand loss of any single principal component without causing interruptions of electricity supply. Today however, N-1 security is challenged, mainly due to reluctance towards new power lines, massive integration of renewable energy sources, and the liberalisation of the electricity market. To deal with this, more intelligence has been introduced into the power system. something that has increased the complexity of the power system [1]. At the same time as N-1 security is challenged, it is also clear that N-1 security is not enough to prevent major events in the power system, as clearly demonstrated by recent blackouts such as in the US/Canada, Sweden/Denmark and Italy in 2003 [2], and the Europe blackout in 2006 [3].

To be able to secure the power system in a cost-effective way, it is important to understand where the system is most vulnerable and what measures will have most effect. Kröger and Zio [4] have provided an overview of approaches for vulnerability assessments of critical infrastructure. All approaches listed require quite detailed knowledge of the system. This is also the case for the quantitative analytical approach commonly taken for risk analysis of electricity supply [5], and for probabilistic modelling that have been pointed out by some as a way to increase cost-effectiveness in the security work [1, 6]. The deep knowledge of the electricity system, detailed computer models and specialized computer tools required makes such approaches difficult to use when also introducing "new" aspects, such as ICT. The models of the power system are already complex, and ICT components are present all the way from the bays to the control centres, constituting a big distributed ICT system. Creating a unified model that is reasonably correct is not easy. There is also a need to estimate failure probabilities of ICT components. Achieving confidence in such estimates is challenging as estimates will have to be made with limited experience data available. Some of the ICT components are relatively new, the introduction of ICT happens fast, and the threat landscape is constantly changing.

Because of the above challenges, there is a need for approaches that can add value also without excessive modelling effort and that can improve understanding of the interdependencies between power and ICT. To that end, this paper:

- contributes to increased mutual understanding between ICT and power experts
- identifies indicators that can be used to monitor trends when it comes to the risk of ICT security incidents in power systems

Currently the interdependencies between the power and ICT system are not fully understood, including how threats (both malicious and accidental) towards the ICT system may impact on power delivery [7, 8]. As a step towards increased understanding of these interdependencies, this paper address cyber security challenges of the transmission system, considering the ICT technology that can be found in such systems today. Though the focus is on the transmission system, many of the issues identified are likely to be also relevant for smarter distribution systems. The use of indicators can increase the Transmission Service Operator's (TSO's) understanding of the effects ICT have on power system security. This

will improve the basis for current decision making at TSOs, especially when it comes to measures needed, and can improve foundations for detailed vulnerability assessments later on.

The paper is organised as follows. Section 2 provides a brief overview of ICT components that are used in power transmission systems today. Section 3 provides an overview of central terms, with a main emphasis on terms that are used differently among ICT and power system experts. Section 4 identifies threats towards ICT systems that may impact power delivery. Section 5 gives an introduction to the role of indicators. Section 6 suggests and evaluates candidate indicators that can be used as a starting point by TSOs. Section 7 discusses the contribution of the paper, and Section 8 concludes the paper.

2 Overview of main ICT components in power transmission systems

The ICT systems used for transmission [9–13] include monitoring, control and regulation systems, protection systems, defence systems, automation systems and communication systems. The transmission system itself is highly distributed and complex. The ICT system is also distributed and dependent on efficient and reliable communication technology. Communication equipment and critical ICT components are usually duplicated.

Wei et al. [13] divide the major functions of power grids into three levels: the corporate level, the control centre level and the substation level. The corporate level is concerned with business and operation management (more long term), while the control centre level and the substation level are involved in the real-time management of the power system. Important functions of the control centre level is forecasting of load and power generation sources, monitoring of system state, operation, system analysis, making recommendations, processing of alarms, training, logging and data exchange. At the substation level, the main functions are to perform normal operation (collecting data and alarms, sending them to the control centre, and executing commands from the control centre), exchange of protection data within the substation, emergency operation, engineering, logging and maintenance.

Typically, the power system is organised in a hierarchical fashion, where substations are under the control of a control centre, that again may be under the control of higher-level control centres [13]. This way you end up with Regional Control Centres (RCCs), National Control Centres (NCCs), and even also transnational control centres. Status information is measured at bay level, collected at substations, and then forwarded to the Supervisory Control and Data Acquisition (SCADA) system. State estimators make the system able to cope with missing or erroneous system variables [11]. The SCADA system and EMS (Energy Management System) provide operators with updated status information, and also the possibility to issue commands. Essential in this respect is the communication infrastructure connecting the control centres with the substa-

tions and their bays. The substations also have control rooms with monitoring and control capabilities.

In addition to the centralised control scheme, the transmission system also consists of a large number of distributed autonomous intelligent devices that take part in ensuring safe and secure operation of the transmission grid. The most important example is represented by the protection devices [14] that have an important role in ensuring any failures have as little impact as possible, e.g. by disconnecting faulty parts of the grid. Protection devices come in different types. Many of them require communication in order to work effectively, and have strict requirements when it comes to response times. Protection devices are usually duplicated at the transmission level.

Lately, more intelligence has been introduced into the power system in form of Special Protection Schemes (SPSs) that are able to implement corrective actions automatically and cover a wider area, and Phase-Shifting Transformers (PSTs) and Static VAR Compensators[4] (SVCs) that increase controllability [1]. Wide-Area Monitoring Systems (WAMS) provide enhanced situational awareness and thus assist in decision making at control centres [11].

It is worth noting that a lot of the components and systems mentioned above, like protections, are not traditionally considered to be ICT. Still, the current development has turned also these devices into small computers that rely on communication. In this paper they are thus considered part of the ICT system.

3 Terms: Communication challenges between ICT and power experts

Properly addressing the ICT risks of the combined ICT and transmission system requires cooperation between people from different disciplines: experts on electric power systems and experts on ICT, people with dependability background, people working on safety, and people with cyber security background. The terms used vary between the different disciplines, with one of the most confusing terms being "security".

3.1 Security, information security and cyber security

In the context of ICT, the work on protecting the systems is usually denoted information security. The key asset to protect is considered to be the information in the systems, and the goal of the information security work is to ensure [15]:

- Confidentiality: *"the property that information is not made available or disclosed to unauthorized individuals, entities, or processes"* [15]
- Integrity: *"the property of safeguarding the accuracy and completeness of assets"* [15]

[4] Volt-Ampere Reactive (VAR) compensators control reactive power injection or absorption in order to improve the performance of the transmission system [11]

– Availability: *"the property of being accessible and usable upon demand by an authorized entity"* [15]

The terms computer security and (ICT) network security[5] are also sometimes used, and when ICT is used in critical infrastructure, the term cyber security is common. The difference between information security, computer security, network security and cyber security is not clearly defined. It can be argued that information security is a broader term as it includes also information not processed, stored or communicated by means of ICT. Computer security and (ICT) network security is more centred on protecting (specific parts of) the ICT technology. Cyber security is focused on the threats coming from closer integration with the Internet, and seems to be primarily used when talking about the security of industrial control systems. The terms are however often used interchangeably, and their definitions are often quite similar. As an example, the NISTIR 7628 guidelines on smart grid cyber security [16] explain cyber security in terms of ensuring confidentiality, integrity and availability of electronic information communication systems. For power systems, however, the term security has a different meaning. According to Kundur et al. [17], *"Security of a power system refers to the degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service."*

3.2 Dependability of ICT systems vs. information security

Dependability of ICT systems can be defined as *"the ability to deliver service that can justifiably be trusted"*, or alternatively *"the ability to avoid service failures that are more frequent and more severe than is acceptable"* [18]. According to Avizienis et al. [18], dependability is comprised of the five attributes: availability, reliability, safety, integrity and maintainability. Thus, dependability and information security have two attributes in common: integrity and availability. These attributes are essential in automation applications. The confidentiality attribute of information security is however not considered for dependability. Traditionally, dependability has been concerned with non-malicious faults while information security has paid attention to the threats posed by malicious actors. There has however for a long time been a growing understanding among the dependability experts that limiting studies to non-malicious faults implies only addressing part of the problem. Among the information security experts, it is evident that also non-malicious faults can cause severe problems for the confidentiality, integrity and availability of information. This is reflected in standards such as ISO/IEC 27005 [19] on information security risk management that specifically states that analyses should include both natural threats and threats with human origin, and also both accidental and deliberate threats. In critical infrastructure protection, the term "all-hazard approach" is often used to emphasise the need to include both natural and man-made events, and also both intentional and unintentional actions [20].

[5] The term 'network' in network security' refers to the ICT network, not the power network.

The terms "hazard" and "threat" have similar meanings. The term *threat* is defined in ISO/IEC 27002 as *"a potential cause of an unwanted incident, which may result in harm to a system or organisation"* [21]. The term *hazard* is defined in IEC 61508 as *"Potential source of harm"* [22]. The term hazard is more commonly used for safety and dependability analysis, whereas the term threat is more commonly used for information security[6].

4 ICT threats relevant for the power system

One step on the way towards a better understanding of the vulnerability that comes from the deep integration of power and ICT systems is to identify the main incidents that may happen in the ICT system, and that may have consequences for power delivery. According to Doorman et al. [23], the major unwanted situations in the energy sector are:

- high price: the price of electricity is higher than usual for a long period
- load curtailment: rationing
- blackouts: interruptions for longer periods of time

As ICT is deeply integrated with the power system, ICT failures may have consequences also along these lines. This is supported by results from the GRID project that identified direct effects ICT system failures may have at the transmission grid level [7]. Among the effects identified were power system instability, loss of generation capacity and loss of lines and/or corridors, malfunction of protection devices or other devices used for power control, and loss of or corrupted observability (e.g. SCADA or EMS).

As outlined in Section 2, the ICT systems used for transmission include monitoring, control and regulation systems, protection systems, defence systems, automation systems and communication systems. According to a survey performed by Gardner et al. [24], industry and research communities agree that the most critical areas are protection and control. This is because of the role that protection and control systems play in normal and abnormal operation, and also the potential consequences of single errors in these types of systems.

The NERC Cyber Attack Force [25] identified a set of cyber attack scenarios for power systems. The cyber attack scenarios were intended to be used as a basis for operational training, and cover the following unwanted situations: social engineering [26] where a false request or false information is sent to an operator; denial of service of EMS network; denial of service of EMS applications; spurious device operations, and; realistic data injection. The cyber attack scenarios listed first are considered more plausible than those listed last.

The different ICT subsystems have different characteristics and may be subject to different types of attacks or failures. Potential threats and vulnerabilities of relevant systems have been documented in several publications. As examples,

[6] Note that some definitions of the term "threat" only include intentional and malicious acts [20].

Wei et al. [13] have identified potential network attacks on typical communication links used for smart grid automation systems, and also the potential adverse impacts of such attacks. In addition, they have identified the main targets of attacks on the SCADA system, including the Front End Processor (FEP), the Human Machine Interface (HMI), the Engineering Workstation (EWS), the database systems, the application server, and the controllers. The National SCADA TestBed (NSTB) [27] has, based on a number of security assessments of SCADA systems, shared information about what types of cyber security vulnerabilities are commonly found in SCADA systems. Sridhar et al. [11] have identified potential cyber vulnerabilities related to state estimation, VAR compensation and Wide-Area Monitoring Systems.

In the following we describe unwanted situations in the ICT system that may cause the effects listed above. The unwanted situations are related to the control and protection area (most critical), and take into account the need for operators to see (observability) what is happening and act (controllability) on what they see. They also consider the potential goal of attackers to influence the state of the system (command injection).

4.1 Loss of or corrupted observability

Loss of or corrupted observability happens in cases where operators, either at a regional or national control centre (RCC/NCC), do not have a correct overview of the current state of the system. This may be due to information not being available (loss of observability) or because of erroneous information in the system (loss of integrity). The consequences of unavailable or erroneous information for the power system can vary from no consequences to high consequences. The consequence is dependent on the degree to which observability is lost or corrupted, i.e. the duration of the incident as well as how much of the system is affected. It is also dependent on the state of the system at the time, and what happens while observability is lost or corrupted. The ability to detect corrupted observability is also important. Consequences may be higher if operators are not aware that information is corrupted, and thus may act on the erroneous state information. Loss of or corrupted observability may happen due to:

- Failure of communication equipment or noise on the communication channel, causing data transmission errors, unavailability of the communication line or excessive delays in the communication
- Failure of central systems at the RCC/NCC, causing the control centre to be unable to communicate or causing unreliable reception of status updates (random modifications)
- Failure of components at the substations, causing the substations to be unable to communicate or causing unreliable status measurements or unreliable processing of status updates at substations
- Attack on the communication ability between RCC and substations
- Injection of false status information

If loss of or corrupted observability is caused by deliberate attackers, this may intentionally hide other malicious activities in the system. Thus, operators are less able to detect the malicious activity and take action. In such cases, the consequences of lacking observability are likely to be higher than when caused by natural failures. False status messages that have been deliberately injected into the system are also more likely to be specifically tailored to trigger specific actions. The total observation of the state of the system may also be changed in a way that seems convincing. Such deliberate corruption of observability by an intelligent adversary is thus more likely to cause major consequences than random failures. Manipulating status information undetected is however very difficult for an attacker, as state estimators verify that the current status information is coherent. To be able to change the state in a coherent way, attackers will require detailed knowledge of the current situations. In addition, attackers must be able to modify all signals and measurements in a coherent way.

4.2 Uncontrollability of the system

Uncontrollability of the system happens in cases where operators of the SCADA system are not able to send commands in order to control the power system. Uncontrollability also happens if the components that act on the commands stop responding to commands or responds in an unintended way due to malfunction or an attack. Also in this case, the consequences are dependent on the duration and extent of the uncontrollability, and the state of the system at the time. Loss of controllability may happen due to:

- Failure of communication equipment or noise on the communication channel, causing data transmission errors, unavailability of the communication line or too high delays in the communication
- Failure of central systems or components at the substations, RCC or NCC, causing the systems to be unable to communicate or causing unreliable sending or reception of messages
- Failure of components that act on commands
- Attack on the communication ability of central systems

If uncontrollability is caused by attackers, as opposed to random failures, the consequences are likely to be more severe as attackers are likely to cause uncontrollability of central components at a time when such control is needed.

4.3 Command injection

Command injection happens if components receive commands that have not been sent by authorised operators. Commands may be injected by attackers that have gained access to system components or the communication channel, but may also happen due to malfunction of equipment. If attackers are able to inject commands that are acted upon (e.g. open/close breakers), they can cause a lot of damage. Though operators are trusted, it is also important to be aware

of the potential of operators to cause harm intentionally or due to mistakes. Attackers may also cause injection of unnecessary and potentially harmful commands indirectly by tricking operators to take unnecessary actions. This may happen due to erroneous information in the system (see Section 4.1) or through social engineering attacks [25].

4.4 Protection system malfunction

Protection systems are essential for power system security, and protection system malfunction may have severe consequences for the power system [28]. Protection system malfunction may be caused by, e.g.:

- Protection systems with incorrect settings, either by mistake or by intent
- No communication or excessive delays in communication between protection systems
- Spurious tripping (caused by technical fault or human error)
- Desynchronized protection systems
- Errors in protection communication, either due to failures or due to modification by a malicious attacker

It is important to be aware that the protection systems operate under strict time conditions, where fault detection, protection decision and isolating device operation must happen in the space of milliseconds [14].

5 An introduction to indicators

The potential unwanted situations described above motivate the need to properly include ICT in work on power system security. As pointed out in the introduction, this is however not trivial and there is a need for improved understanding on the role ICT actually plays and how to properly grasp this in power security analyses. Using indicators is one way to increase understanding.

An indicator is a measurable and operational variable that can be used to describe the condition of a broader phenomenon or aspect of reality [29]. The word indicator comes from the verb *indicate*, which means to designate or to show. An indicator gives a simplified signal of a condition or change in condition, and indicators are typically used when the phenomenon itself is too complicated or too expensive to measure directly. The typical properties of indicators are [30]:

- They provide numerical values (a number or a ratio).
- The indicators are easily updated at regular intervals.
- They only cover some selected determinants of overall safety, security or risk, in order to have a manageable set.

Both individual indicators and their combinations can be useful since one can create a simplified description of the vulnerability level in the system and assess the expected performance and its development. Indicators can be used to see

the long-term evolution (trends over months or even years), but also to observe sudden changes. Indicators can be characterised as leading (proactive, i.e., things that happen before an incident) or lagging (reactive, i.e., things that happen as a cause of or after an incident).

Table 1. Overview of approaches to identify indicators

Approach	*Description*
Risk based methods [29, 31]	Utilize a risk model as a basis. This is usually an existing risk model, but the development of a risk model may also be part of the method.
Safety performance based methods [32–35]	Start from a set of influencing factors assumed to be important to safety.
Incident based methods [36]	Identifies indicators by an in-depth study of one or more incidents or accidents.
Resilience based methods [37]	Identify indicators of human and organisational performance in a resilience perspective

Table 1 provide an overview of existing approaches for developing indicators. *Risk based methods* are based on the hypothesis that risk control can be achieved through the control of risk influencing factors (RIFs), which are those factors having effect on risk. The conditions for this hypothesis to be true are that 1) All relevant RIFs are identified, 2) The RIFs are measurable and 3) The relationship between RIFs and risk is known. *Safety performance* indicators are based on important factors, but they are not related to a risk analyses. This also applies to *incident based methods* and *resilience based methods*. The resilience based method differs from the others by focusing on positive signals ("what went right" and why), rather than failures ("what went wrong").

The methods differ in scope and depth of analysis. The risk based approaches will cover the whole installation and all risks, since these methods narrow the focus to the most important risk factors. The resilience based approach can in principle also cover a complete installation with all its risks. The performance based methods will usually narrow the scope to certain systems or activities. The incident based methods will usually only cover specific systems and not a complete installation, but may go deeper into an area or system, which the other methods perhaps will not cover. Also, with the risk based methods it is easy to determine the risk significance, including relative risk importance between the various risk influencing factors. A main weakness with the other methods is that the risk significance and the relative importance of influencing factors or causes are unknown.

The literature describes a number of desirable properties for an indicator; but in practice, it appears very challenging to find indicators that meet all the requirements which are desirable. Below we list a selection of criteria for good indicators [38–42]:

- *Relevance (meaning):* The indicator value is assumed to be (strongly) correlated with either event frequency or consequence; or possibly with influencing factors or important parameters of a risk or vulnerability model; e.g. with Risk Influencing Factors (RIFs) of an influence diagram.
- *Availability:* Data to calculate the indicator can be acquired at a reasonable cost.
- *Reliability:* Data measured is regarded as being objective and without significant sources of error.
- *Completeness:* The total set of indicators should be complete, i.e. should cover all major types of hazards and system vulnerabilities.
- *Ownership:* A sense of "ownership" should be instilled in the users of the indicators (this is hopefully a consequence of the other criteria).

6 Cyber security indicators for TSOs: An initial set

To assess the vulnerability of the complete power and ICT system, it would be beneficial to create a risk model of the power system incorporating the ICT aspects, where all risk influencing factors are identified and measureable, and the relationships between the risk influencing factors are known. Risk indicators can then be used to describe the condition of risk influencing factors. However, it is very challenging to achieve this, because of the complexity of the system and the dynamics of an incident; there are many potential courses of events following a single incident, and human and organisational factors play a vital part in deciding how the skein will unravel. Furthermore, new types of threats and attacks are constantly emerging, and there is a lack of historical experience data. It is a challenge to estimate the contribution of human and organisational factors to the risk in a system. Detailed risk calculations will give results with considerable uncertainty due to the uncertainty related to such risk modelling, estimation of risk influencing factors, the relationships between them and lack of data.

Due to the current limited understanding of how ICT influences power system security, we have chosen to use a more simple approach to identifying indicators in this work. The literature describes several metrics that can be useful to measure trends of risk influencing factors [43–45, 37]. Based on this literature we have selected a set of indicators which can be relevant to improve understanding of the risk related to ICT incidents for transmission systems. About half of the indicators are based on indicators suggested by Gelbstein [45] (I3-5, I8, I13-14, I16, I18-20 in Table 2) and the rest were identified during a workshop with four experts on ICT, power systems and the use of indicators (I2, I6-7, I9-11, I17) or in discussions with colleagues before the workshop (I1, I12, I15). In the workshop all identified indicators were assessed based on their relevance, availability and reliability.

The selection of indicators has the following limitations:

- The hazards/threats mainly cover malicious attacks (security), but dependability issues (hardware and software problems) are also considered.

– A variant of a safety performance based method is used in the development of indicators, i.e. identifying indicators from factors that influence the security based on literature and expert knowledge.
– The identified indicators must be considered as examples, not an exhaustive list.
– The indicators are numerical values, monitored automatically or easily updated at regular intervals.

The factors and conditions that are taken into account and that may influence the security of the transmission systems are: threats to the ICT system, unwanted events, the performance of barriers of the ICT system, availability of the ICT system, and resilience of the TSO's organisation. An overview of the indicators and their evaluation score, as regards relevance (C1), availability (C2) and reliability (C3), is shown in Table 2. Scores were given from 1-5, where 5 is best.

7 Discussion

Today, the electrical power system is strongly dependent on ICT. Common cause failures can affect both infrastructures due to location-specific and functional interdependencies. There is a need to analyse how power systems and ICT interact and depend on each other, and these insights are lost if the technologies from these two disciplines are only studied separately. For efficient cooperation between power system and ICT experts, it is however crucial to take into account the difference in culture and use of terms in the two disciplines.

The combined power and ICT system is complex and highly distributed. Existing methods for vulnerability analysis often require quite explicit and detailed knowledge of the system. Currently, such deep knowledge is not available when it comes to the interrelations between power systems and ICT. There is thus a need to improve the understanding of the role of ICT, including the potential consequences of unwanted ICT incidents when it comes to power delivery. In this paper we contribute towards this by providing an overview of potential ICT incidents that may have such consequences. We also propose an initial set of indicators that can be used to monitor and improve understanding of the security of the ICT components and their influence on power system security.

It is not possible to measure the safety, security or vulnerability of such a complex system directly. Indicators can be used to measure factors that are important for the vulnerability of a system, and particularly the trends associated with such factors. In a complex system, there are several such factors and thus a high number of potential indicators. Still, it is important to have a manageable set of indicators that can be regularly monitored and followed up. The indicators suggested in this paper represent a first step towards identifying relevant indicators for TSOs that wish to monitor ICT risks and their impact on power security. Further work should include further identification, evaluation and testing of indicators, and should examine more carefully the interrelations and coverage of the suggested indicators.

Table 2. Overview of indicators; C1 = Relevance, C2 = Availability, C3 = Reliability

Influencing factor	***Indicator***	***C1***	***C2***	***C3***
Threats	I1: Measurement describing the network traffic	3	5	5
	I2: Number of events (e.g. number of malicious attacks) of a certain type during e.g. the last month	5	2	2
	I3: Number of attempted intrusions detected [45]	4	2	2
Unwanted events	I4: Number of successful intrusion detected [45]	4	4	5
Barriers	I5: Number of orphaned accounts for access to sensitive information or critical systems [45]	4	4	3
	I6: Percentage share of identified software vulnerabilities not patched	4	3	3
	I7: Number of former employees still having access	4	5	4
Availability	I8: Total downtime (per critical ICT system) in the period reported (planned and not planned) [45]	3	5	4
	I9: Total downtime in the power system due to ICT interruptions in the period reported (planned and not planned)	4	5	4
	I10: Number of interruptions with downtime in the ICT system (operation regularity)	3	5	4
	I11: Number of interruptions with downtime in the power system due to ICT (operation regularity)	5	4	3
Resilience	I12: Proportion of personnel (%) working in ICT-systems with formal expertise in ICT	4	4	3
	I13: Number of unfilled positions in the ICT organisation [45]	3	4	4
	I14: Number of “near misses” in information security activities where no incident occurred, but could happen with small changes in the events [45]	5	1	2
	I15: Time from a vulnerability is reported to feedback is given	1	4	3
	I16: Mean time required to close a reported critical security incident [45]	4	4	3
	I17: Number of reported critical security incident not handled (backlog)	4	4	4
	I18: Number of related critical audit recommendations that have not been implemented [45]	4	4	5
	I19: Number of high impact items registered where mitigation activities have not been completed [45]	4	4	4
	I20: Number of information security processes or activities carried out by a single individual for whom there is no immediate backup or replacement [45]	4	2	2

The usefulness of indicators depend on how they are used in the organisation. An indicator or a combination of indicators with values outside the predetermined acceptable limits usually require actions. Input from indicators can also be used in deciding whether additional measures are necessary.

8 Conclusion

Terminology is a challenge in a multidisciplinary field, and best results are achieved when terms are explicitly defined. Many information security challenges can affect power transmission systems, and using indicators is a promising way to work proactively with information security in a traditionally safety-oriented domain.

Acknowledgments

The work has been done as part of the AFTER project funded by EU, grant. nr. 267188. The authors would like to thank the other partners in this project for their cooperation, and especially the Coordinator Emanuele Ciapessoni from RSE.

References

1. Panciatici, P., Bareux, G., Wehenkel, L.: Operating in the fog: Security management under uncertainty. Power and Energy Magazine, IEEE **10**(5) (2012) 40–49
2. Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., Vittal, V.: Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. IEEE Transactions on Power Systems **20**(4) (2005) 1922–1928
3. Union for the Coordination of Transmission of Electricity (UCTE): Final report - system disturbance on 4 november 2006 (2007)
4. Kröger, W., Zio, E.: Vulnerable Systems. 1st edn. Springer Publishing Company, Incorporated (2011)
5. Kjølle, G., Gjerde, O.: Risk analysis of electricity supply. In Hokstad, P., Utne, I.B., Vatn, J., eds.: Risk and Interdependencies in Critical Infrastructures. Springer Series in Reliability Engineering. Springer London (2012) 95–108
6. Ciapessoni, E., Cirio, D., Grillo, S., Massucco, S., Pitto, A., Silvestro, F.: Operational risk assessment and control: A probabilistic approach. In: Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES. (2010) 1–8
7. The GRID consortium: ICT Vulnerabilities of Power Systems: A Roadmap for Future Research (October 2007)
8. Hokstad, P., Utne, I.B., Vatn, J., eds.: Risk and Interdependencies in Critical Infrastructures – A Guideline for Analysis. Springer Series in Reliability Engineering. Springer
9. Egozcue, E., Rodríguez, D.H., Ortiz, J.A., Villar, V.F., Tarrafeta, L.: Smart Grid Security, Anex I. General Concepts and Dependencies with ICT. Technical Report Deliverable - 2012-04-19, ENISA (2012)

10. Wang, W., Xu, Y., Khanna, M.: A survey on the communication architectures in smart grid. Computer Networks **55**(15) (2011) 3604 – 3629
11. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber physical system security for the electric power grid. Proceedings of the IEEE **100**(1) (2012) 210–224
12. MIT: The Future of the Electric Grid. An Interdisciplinary MIT Study. (December 2011)
13. Wei, D., Lu, Y., Jafari, M., Skare, P., Rohde, K.: Protecting smart grid automation systems against cyberattacks. IEEE Transactions on Smart Grid **2**(4) (2011) 782–795
14. Mesbah, M., Samitier, C., Einarsson, T., Acacia, M., Alvarez, J., Carmo, U., Castro, F., Cimadevilla, R., Darne, J., Dollerup, S., Freitas, J., Komatsu, C., Leroy, T., Ordunez, M.A., Runesson, A., Spiess, H., Stockton, M., Struecker, A., Valente, M., Vianello, G., Viziteu, I., Wright, J.: Line and system protection using digital circuit and packet communication. Technical Report JWG D2B5.30, CIGRE (2012)
15. ISO/IEC 27001:2005: Information technology - security techniques - information security management systems - requirements
16. The Smart Grid Interoperability Panel - Cyber Security Working Group: NISTIR 7628: Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture and high-level requirements (2010)
17. Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., Van Cutsem, T., Vittal, V.: Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. IEEE Transactions on Power Systems **19**(3) (2004) 1387–1401
18. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing **1**(1) (2004) 11–33
19. ISO/IEC 27005:2008: Information technology - Security techniques - Information security risk management
20. Zio, E., Piccinelli, R., Sansavini, G.: An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures. In: Proceedings of the European Safety and Reliability Conference 2011, Troyes, France (September 2011) 2451–2458
21. ISO/IEC 27002:2005: Information technology - security techniques - code of practice for information security management
22. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
23. Doorman, G., Uhlen, K., Kjølle, G., Huse, E.: Vulnerability analysis of the nordic power system. IEEE Transactions on Power Systems **21**(1) (2006) 402–410
24. Gardner, R., Consortium, G.: A survey of ICT vulnerabilities of power systems and relevant defense methodologies. In: Power Engineering Society General Meeting, 2007. IEEE. (2007) 1–8
25. NERC: Cyber Attack Task Force, Final Report (May 2012)
26. Orgill, G.L., Romney, G.W., Bailey, M.G., Orgill, P.M.: The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: Proceedings of the 5th conference on Information technology education. CITC5 '04, New York, NY, USA, ACM (2004) 177–181
27. National SCADA Test Bed (NSTB): Common Cyber Security Vulnerabilities Observed in Control System aSsessments by the INL NSTB Program. Technical Report INL/EXT-08-13979, Idaho National Laboratory (November 2008)

28. Kjølle, G., Gjerde, O., Hjartsjø, B., Engen, H., Haarla, L., Koivisto, L., Lindblad, P.: Protection system faults – a comparative review of fault statistics. In: International Conference on Probabilistic Methods Applied to Power Systems, 2006. PMAPS 2006. (2006) 1–7
29. Øien, K.: Risk indicators as a tool for risk control. Reliability Engineering & System Safety **74**(2) (2001) 129 – 145
30. Øien, K., Utne, I., Herrera, I.: Building safety indicators: Part 1 theoretical foundation. Safety Science **49**(2) (2011) 148 – 161
31. Vinnem, J., Bye, R., Gran, B., Kongsvik, T., Nyheim, O., Okstad, E., Seljelid, J., Vatn, J.: Risk modelling of maintenance work on major process equipment on offshore petroleum installations. Journal of Loss Prevention in the Process Industries **25**(2) (2012) 274 – 292
32. UK Health and Safety Executive (HSE): Development process safety indicators. a step-by-step guide for chemical and major hazard industries (2003)
33. Centre for Chemical Process Safety (CCPS): Process safety leading and lagging metrics. you dont improve what you dont measure (2008)
34. Organisation for Economic Cooperation and Development (OECD): Guidance on developing safety indicators related to chemical accident prevention, preparedness and response. OECD Environment, Health and Safety Publications, Series on Chemical Accidents, no. 19 (2008)
35. Electric Power Research Institute (EPRI): Final report on leading indicators of human performance (2001)
36. Øien, K.: Development of early warning indicators based on accident investigation. In: PSAM9 International Probabilistic Safety Assessment and Management Conference. (May 2008)
37. Øien, K., Massaiu, S., Tinmannsvik, R., Strseth, F.: Development of early warning indicators based on resilience engineering. In: PSAM10 International Probabilistic Safety Assessment and Management Conference. (June 2010)
38. Rockhwell, T.: Safety performance measurement. Journal of Industrial Engineering **10** (1959) 12–16
39. Kjellén, U.: The safety measurement problem revisited. Safety Science **47** (2009) 486–489
40. Kjellén, U.: Prevention of Accidents through Experience Feedback. Taylor & Francis, London, NY (2000)
41. Vinnem, J.E.: Risk indicators for major hazards on offshore installations. Safety Science **48**(6) (2010) 770 – 787
42. Herrera, I.A., Hollnagel, E., Håbrekke, S.: Proposing safety performance indicators for helicopter offshore on the norwegian continental shelf. In: 10th International Probabilistic Safety Assessment & Management Conference(PSAM 10). (2010)
43. SANS Institute: Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG), version 3.1 (October 2011)
44. Herrmann, D.S.: Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience and ROI. Auerbach Publications, Taylor & Francis Group, New York (2007)
45. Gelbstein, E.E.: Designing a Security Audit Plan for a Critical Information Infrastructure (CII). In Laing, C., Badii, A., Vickers, P., eds.: Securing Critical Infrastructures and Critical Control Systems: Approaches for threat Protection. IGI Global (May 2013) 262–285